Fundamental Concepts of Mathematics

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 215

Subsection 1

Functions

Definition of Function

- Intuitively, a function is a "rule" or "mechanism" that transforms one quantity into another.
- Example: The function $f(x) = x^2 + 4$ takes an integer x and transforms it into the integer $x^2 + 4$. The function $g(x) = |x|$ takes the integer x and returns x if $x \geq 0$ and $-x$ if $x < 0$.

Definition of Function

A **function** is a relation f that satisfies $(a, b) \in f$ and $(a, c) \in f$ imply $b = c$.

- Equivalently, a relation f is not a function if there exist a, b, c with $(a, b) \in f$ and $(a, c) \in f$, and $b \neq c$.
- Example: Let $f = \{(1, 2), (2, 3), (3, 1), (4, 7)\}$ and $g = \{(1, 2), (1, 3), (4, 7)\}$.
  The relation f is a function. The relation g is not because $(1, 2), (1, 3) \in g$ and $2 \neq 3$.

Ordinary Function Notation $F(\bullet)$

- When expressed as a set of ordered pairs, functions do not look like rules for transforming one object into another. However, the ordered pairs in f associate "input" values (the first elements in the lists in f) with "output" values (the second elements in the lists).
- What makes f a function is that for each input there can be at most one output.
- We rarely use the notation $(1, 2) \in f$, even though this is formally correct. Instead, we use the $f(\bullet)$ notation:

Function Notation

Let f be a function and let a be an object. The notation $f(a)$ is defined provided there exists an object b such that $(a, b) \in f$. In this case, $f(a)$ equals b. Otherwise, $f(a)$ is undefined.

Function Notation: An Example

- Express the integer function $f(x) = x^2$ as a set of ordered pairs.

  We might use list notation:

  $$f = \{\ldots, (-3, 9), (-2, 4), (-1, 1), (0, 0), (1, 1), (2, 4), (3, 9), \ldots\}.$$

  It is much clearer if we use set-builder notation:

  $$f = \{(x, y) : x, y \in \mathbb{Z}, y = x^2\}.$$

The Domain and the Image of a Function

Domain and Image

Let f be a function. The set of all possible first elements of the ordered pairs in f is called the **domain of** f and is denoted $\text{dom}f$. The set of all possible second elements of the ordered pairs in f is called the **image of** f and is denoted $\text{im}f$.

- In logical notation

$$\text{dom}f = \{a : \exists b, (a, b) \in f\} \quad \text{and} \quad \text{im}f = \{b : \exists a, (a, b) \in f\}.$$

- Example: Let $f = \{(1, 2), (2, 3), (3, 1), (4, 7)\}$. Then $\text{dom}f = \{1, 2, 3, 4\}$ and $\text{im}f = \{1, 2, 3, 7\}$.
- Example: Let f be the function $f = \{(x, y) : x, y \in \mathbb{Z}, y = x^2\}$. The domain of f is $\mathbb{Z}$ and the image of f is the set of all perfect squares.

Functions from A to B

A Function from A to B

Let f be a function and let A and B be sets. We say that f is a **function from A to B** provided $\text{dom} f = A$ and $\text{im} f \subseteq B$. In this case, we write $f : A \to B$. We also say that f is a **mapping from A to B**.

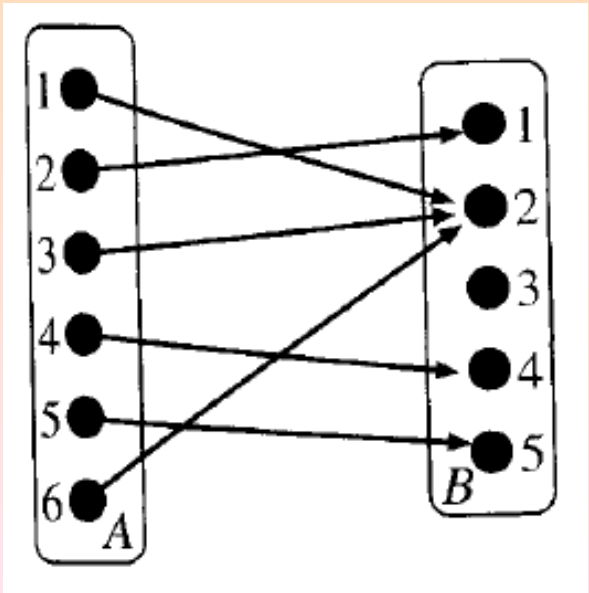
- So we have $f : A \to B$ if
  - f is a function;
  - $\text{dom} f = A$;
  - $\text{im} f \subseteq B$.
- Example: Consider the sine function. It is defined for every real number and returns a real value. The domain of the sine function is $\mathbb{R}$ and the image is $[-1, 1]$. Thus, we can write $\sin : \mathbb{R} \to \mathbb{R}$. Is it correct to write $\sin : \mathbb{R} \to [-1, 1]$?

Graphs of Functions from $\mathbb{R}$ to $\mathbb{R}$

- To draw the graph of a function whose inputs and outputs are real numbers, we plot a point in the plane at coordinates $(x, f(x))$, for every $x \in \text{dom} f$.
- Formally, the graph of a function is the set $\{(x, y) : y = f(x)\}$. Thus, to speak of "the graph of a function" is redundant because it actually is the function!
- To verify that a picture represents a function from reals to reals, we can apply the vertical line test: Every vertical line in the plane may intersect the graph of a function in at most one point.
- If a vertical line hit the graph twice we would have two different points (x, y_1) and (x, y_2), both on the graph, i.e., such that $(x, y_1), (x, y_2) \in f$ with $y_1 \neq y_2$, which is forbidden by the definition of function.

Functions $f : A \to B$ with A, B Finite I

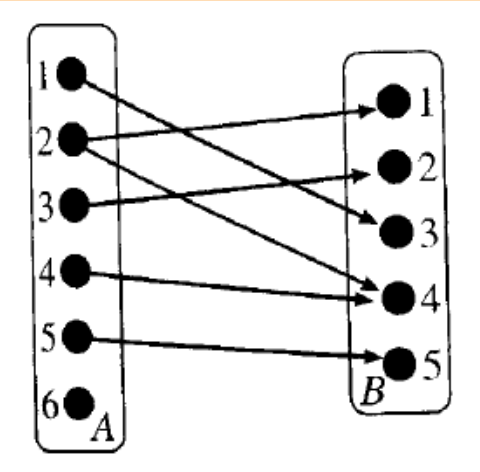
- Let $A = \{1, 2, 3, 4, 5, 6\}$ and $B = \{1, 2, 3, 4, 5\}$ and consider the function $f : A \to B$ defined by $f = \{(1, 2), (2, 1), (3, 2), (4, 4), (5, 5), (6, 2)\}$. A picture of f is created by drawing two sets of dots: one for A on the left and one for B on the right. We draw an arrow from a dot $a \in A$ to a dot $b \in B$ just when $(a, b) \in f$, i.e., $f(a) = b$.



The picture, makes it easy to see that $\text{im} f = \{1, 2, 4, 5\}$.

Functions $f : A \to B$ with A, B Finite II

- Now consider g defined by $g = \{(1,3),(2,1),(2,4),(3,2),(4,4),(5,5)\}$. Let $A = \{1,2,3,4,5,6\}$ and $B = \{1,2,3,4,5\}$. Then $g : A \to B$ is false.



- First, $6 \in A$ but $6 \notin \text{dom}g$. Thus $\text{dom}g \neq A$. In the picture, there are no arrows emanating from element 6.
- Second, g is not a function (from any set to any set). Notice that $(2,1),(2,4) \in g$. In the picture, there are two arrows emanating from element 2.
- If f is a function from A to B ($f : A \to B$), its picture satisfies the condition:

Every dot on the left (in A) has exactly one arrow leaving it, ending at the right (in B).

Number of Functions

Proposition

Let A and B be finite sets with $|A| = a$ and $|B| = b$. The number of functions from A to B is b^a.

- Choose $A = \{1, 2, \ldots, a\}$ and $B = \{1, 2, \ldots, b\}$.
  Every function $f : A \to B$ can be written out as

$$f = \{(1, ?), (2, ?), (3, ?), \ldots, (a, ?)\},$$

  where the ? entries are elements from B. In how many ways can we replace the ?s with elements in B?
  There are b choices for the element ? in $(1, ?)$, and for each such choice, there are b choices for the ? in $(2, ?)$, etc., and finally b choices for the ? in $(a, ?)$ given all the previous choices. Thus, all told, there are $\underbrace{b \cdot b \cdot \cdots \cdot b}_{a \text{ times}} = b^a$ choices.

An Example

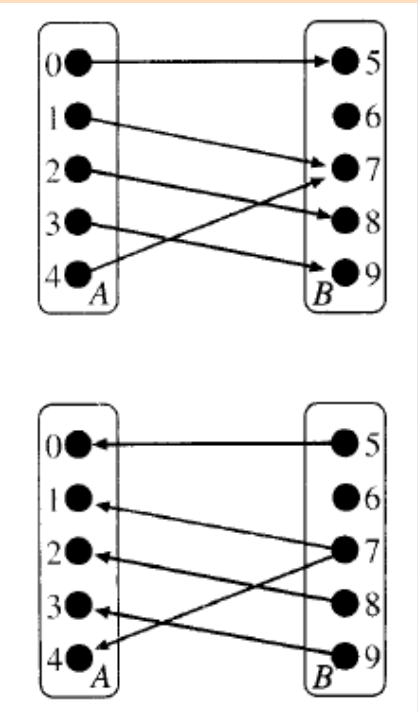
- Let $A = \{1, 2, 3\}$ and $B = \{4, 5\}$. Find all functions $f : A \to B$.

  The Proposition tells that there are $2^3 = 8$ such functions. They are

$$\begin{array}{ll} \{(1,4),(2,4),(3,4)\} & \{(1,5),(2,4),(3,4)\} \\ \{(1,4),(2,4),(3,5)\} & \{(1,5),(2,4),(3,5)\} \\ \{(1,4),(2,5),(3,4)\} & \{(1,5),(2,5),(3,4)\} \\ \{(1,4),(2,5),(3,5)\} & \{(1,5),(2,5),(3,5)\} \end{array}$$

Inverse Relations of Functions

- We defined the **inverse** of a relation R, denoted R^{-1} as the relation formed from R by reversing all its ordered pairs.
- Since a function f is a relation, we may also consider f^{-1}.
- If f is a function from A to B, is f^{-1} a function from B to A?
- Example:



Let $A = \{0, 1, 2, 3, 4\}$ and $B = \{5, 6, 7, 8, 9\}$. Let $f : A \to B$ be defined by

$$f = \{(0, 5), (1, 7), (2, 8), (3, 9), (4, 7)\}.$$

Then

$$f^{-1} = \{(5, 0), (7, 1), (8, 2), (9, 3), (7, 4)\}.$$

So f^{-1} is not a function from B to A.

- First, f^{-1} is not a function.
- Second, $\text{dom} f^{-1} = \{5, 7, 8, 9\} \neq B$.

One-to-one Functions

Definition of One-to-one Functions

A function f is called **one-to-one** provided that, whenever $(x, b), (y, b) \in f$, we must have $x = y$. Equivalently, if $x \neq y$, then $f(x) \neq f(y)$.

Proposition

Let f be a function.

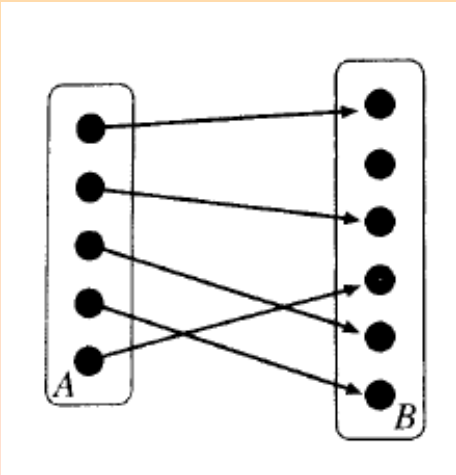
- The inverse relation f^{-1} is a function if and only if f is one-to-one.
- If f^{-1} is also a function, then $\text{dom} f = \text{im} f^{-1}$ and $\text{im} f = \text{dom} f^{-1}$.

- f^{-1} is a function iff $((b, x), (b, y) \in f^{-1}$ imply $x = y)$ iff $((x, b), (y, b) \in f$ imply $x = y)$ iff f is one-to-one.
- $\text{im} f^{-1} = \{a \in A : \exists b \in B, (b, a) \in f^{-1}\} = \{a \in A : \exists b \in B, (a, b) \in f\} = \text{dom} f$. Similarly for $\text{im} f = \text{dom} f^{-1}$.

Methods for Proving a Function is One-to-one

- Three methods to show f is one-to-one:
  - Direct method: Suppose $f(x) = f(y)$. Prove that $x = y$.
  - Contrapositive method: Suppose $x \neq y$. Show that $f(x) \neq f(y)$.
  - Contradiction method: Suppose $f(x) = f(y)$ but $x \neq y$. Derive a contradiction!
- Example: Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = 3x + 4$. Prove that f is one-to-one.
  Suppose $f(x) = f(y)$. Then $3x + 4 = 3y + 4$. Subtracting 4 from both sides gives $3x = 3y$. Dividing both sides by 3 gives $x = y$. Therefore f is one-to-one.
- To prove that a function is not one-to-one requires us to present a counterexample, i.e., objects x and y with $x \neq y$ but $f(x) = f(y)$.
- Example: Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = x^2$. Prove that f is not one-to-one.
  Notice that $f(3) = f(-3) = 9$, but $3 \neq -3$. Therefore f is not one-to-one.

Onto Functions

- Let $f : A \to B$. When is f^{-1} is a function from B to A?
  - First, f^{-1} needs to be a function.
  - Second, every element in B must have an incoming arrow.
- 

Consider $f : A \to B$ shown in the figure.
  - Clearly f is one-to-one, so f^{-1} is a function.
  - However, f^{-1} is not a function from B to A because there is an element $b \in B$ for which $f^{-1}(b)$ is undefined. For $f^{-1} : B \to A$, there must be an f-arrow pointing to every element of B.

Definition of Onto Function

Let $f : A \to B$. We say that f is **onto** B provided that for every $b \in B$ there is an $a \in A$ so that $f(a) = b$. Equivalently, $\text{im} f = B$.

- The sentence "$f : A \to B$ is onto" is a promise that (a) f is a function; (b) $\text{dom} f = A$; and (c) $\text{im} f = B$.

Example

- Let $A = \{1, 2, 3, 4, 5, 6\}$ and $B = \{7, 8, 9, 10\}$. Let

$$\begin{aligned} f &= \{(1,7),(2,7),(3,8),(4,9),(5,9),(6,10)\} \\ g &= \{(1,7),(2,7),(3,7),(4,9),(5,9),(6,10)\}. \end{aligned}$$

  $f : A \to B$ is onto because for each element b of B, we can find one or more elements $a \in A$ such that $f(a) = b$. Equivalently, it is easy to check that $\text{im} f = B$.
  $g : A \to B$ is not onto. Note that $8 \in B$, but there is no $a \in A$, with $g(a) = 8$. Also, $\text{im} g = \{7, 9, 10\} \neq B$.
- The condition that $f : A \to B$ is onto can be expressed using the quantifiers: $\forall b \in B, \exists a \in A, f(a) = b$.
- The condition that $f : A \to B$ is not onto can be similarly expressed: $\exists b \in B, \forall a \in A, f(a) \neq b$.

Proving a Function is Onto

- To show $f : A \to B$ is onto:
  - Direct method: Let b be an arbitrary element of B. Explain how to find/construct an element $a \in A$ such that $f(a) = b$.
  - Set method: Show that the sets B and im$f$ are equal.
- Example: Let $f : \mathbb{Q} \to \mathbb{Q}$ be defined by $f(x) = 3x + 4$. Prove that f is onto $\mathbb{Q}$.

  Let $b \in \mathbb{Q}$ be arbitrary. We seek an $a \in \mathbb{Q}$, such that $f(a) = b$. By *reverse engineering*, let $a = \frac{b-4}{3}$. Since b is a rational number, so is a. Moreover,

$$f(a) = 3\frac{b-4}{3} + 4 = (b-4) + 4 = b.$$

  Therefore $f : \mathbb{Q} \to \mathbb{Q}$ is onto.

Invertibility of Functions

Theorem (Invertibility of Functions)

Let A and B be sets and let $f : A \to B$. The inverse relation f^{-1} is a function from B to A if and only if f is one- to-one and onto B.

- Let $f : A \to B$.
  - Suppose, first, f is one-to-one and onto B. We need to prove that $f^{-1} : B \to A$.
    By a previous proposition, we get f^{-1} is a function, since f is one-to-one, $\text{dom} f^{-1} = \text{im} f \overset{\text{onto}}{=} B$ and $\text{im} f^{-1} = \text{dom} f = A$. Therefore, $f^{-1} : B \to A$.
  - Suppose $f : A \to B$ and $f^{-1} : B \to A$. Since f^{-1} is a function, f is one-to-one. Since $\text{im} f = \text{dom} f^{-1} = B$, we see that f is onto B.

Bijections

Definition of Bijection

Let $f : A \to B$. We call f a **bijection** provided it is both one-to-one and onto.

- Example: Let A be the set of even integers and let B be the set of odd integers. The function $f : A \to B$ defined by $f(x) = x + 1$ is a bijection.

  We must prove that f is both one-to-one and onto.
  - To see that f is one-to-one, suppose $f(x) = f(y)$ where x and y are even integers. Thus, $f(x) = f(y) \Rightarrow x + 1 = y + 1 \Rightarrow x = y$. Hence f is one-to-one.
  - To see that f is onto B, let $b \in B$ (i.e., b is an odd integer). By definition, $b = 2k + 1$ for some integer k. Let $a = 2k$. Clearly, a is even, i.e., $a \in A$. Moreover, $f(a) = a + 1 = 2k + 1 = b$, so f is onto.

  Since f is both one-to-one and onto, f is a bijection.

Some More Counting of Functions

- Let A and B be finite sets with $|A| = a$ and $|B| = b$. How many functions $f : A \to B$ are one-to-one and how many are onto?
  - If $|A| > |B|$, then f cannot be one-to-one. This happens, since, if f is one-to-one, for distinct elements $x, y \in A$, $f(x)$ and $f(y)$ are distinct elements of B.
  - If $|A| < |B|$, then f cannot be onto. In this case, there are not enough elements in A to "cover" all the elements in B!

Proposition (Pigeonhole Principle)

Let A and B be finite sets and let $f : A \to B$. If $|A| > |B|$, then f is not one-to-one. If $|A| < |B|$, then f is not onto.

- Stated in the contrapositive,
  - if $f : A \to B$ is one-to-one, then $|A| \leq |B|$;
  - if $f : A \to B$ is onto, then $|A| \geq |B|$.

Proposition

Let A and B be finite sets and $f : A \to B$. If f is a bijection, $|A| = |B|$.

Counting One-to-one and Onto Functions

Theorem

Let A and B be finite sets with $|A| = a$ and $|B| = b$.

1. The number of functions from A to B is b^a.
2. If $a \leq b$, the number of one-to-one functions $f : A \to B$ is $(b)_a = b(b-1)\cdots(b-a+1) = \frac{b!}{(b-a)!}$.
   If $a > b$, the number of such functions is zero.
3. If $a \geq b$, the number of onto functions $f : A \to B$ is $\sum_{j=0}^{b}(-1)^j\binom{b}{j}(b-j)^a$. If $a < b$, the number of such functions is zero.
4. If $a = b$, the number of bijections $f : A \to B$ is $a!$.
   If $a \neq b$, the number of such functions is zero.

- If $A = \{1, 2, \ldots, a\}$ and $B = \{1, 2, \ldots, b\}$, a one-to-one function from A to B is of the form $f = \{(1, ?), (2, ?), (3, ?), \ldots, (a, ?)\}$ where the ?s are filled in with elements of B without repetition.
- For counting onto functions, we want to fill in the ?s with elements of B so that every element is used at least once.

Subsection 2

The Pigeonhole Principle

The Pigeonhole Principle

- If A and B are finite sets with $|A| > |B|$, then there can be no one-to-one function $f : A \to B$.
- This is called the Pigeonhole Principle, since, if p pigeons try to occupy h coop holes, then
  - if $p \leq h$, then the coop is large enough so that pigeons do not have to share holes;
  - if $p > h$, then there are not enough holes for private quarters for all.

Proposition

Let $n \in \mathbb{N}$. Then, there exist positive integers a and b, with $a \neq b$, such that $n^a - n^b$ is divisible by 10.

- We use the fact that a natural number is divisible by 10 if and only if its last digit is a zero. Consider the 11 natural numbers $n^1, n^2, \ldots, n^{11}$. The ones digits of these numbers take on values in the set $\{0, 1, 2, \ldots, 9\}$. Since there are only ten possible ones digits, and we have 11 different numbers, two of these numbers (say n^a and n^b) must have the same ones digit. Therefore, $n^a - n^b$ is divisible by 10.

A Geometric Application

- A point whose coordinates are both integers is called a **lattice point**.

Proposition

Given five distinct lattice points in the plane, at least one of the line segments determined by these points has a lattice point as its midpoint.

- We are given five distinct lattice points in the plane. The various coordinates are integers and hence are either even or odd. Given a lattice point's coordinates, we can classify it as one of four types:

$$(\text{even}, \text{even}), \quad (\text{even}, \text{odd}), \quad (\text{odd}, \text{even}), \quad (\text{odd}, \text{odd}).$$

Since we have five lattice points, but only four parity categories, by the Pigeonhole Principle, two of these points must have the same parity type. Suppose these two points have coordinates (a, b) and (c, d). The midpoint of this segment has coordinates $(\frac{a+c}{2}, \frac{b+d}{2})$. Since a and c have the same parity, $a + c$ is even, and so $\frac{a+c}{2}$ is an integer. Likewise, $\frac{b+d}{2}$ is an integer. Therefore, the midpoint is a lattice point.

Sequences and Monotone Subsequences

- A **sequence** is simply a list.
- Given a sequence of integers, a **subsequence** is a list formed by deleting elements from the original list and keeping the remaining elements in the same order in which they originally appeared.
- Example: The sequence

  $$9 \quad 10 \quad 8 \quad 3 \quad 7 \quad 5 \quad 2 \quad 6 \quad 4$$

  contains the subsequence $9 \quad 8 \quad 6 \quad 4$. Notice that the four numbers in the subsequence are in decreasing order. So, we call it a **decreasing subsequence**. Similarly, a subsequence whose elements are in increasing order is called an **increasing subsequence**.
- We claim that every sequence of ten distinct integers must contain a subsequence of four elements that is either increasing or decreasing. The sequence above has a decreasing subsequence of length four and also an increasing subsequence of length four.

Theorem of Erdős and Szekeres

- Example: The sequence

$$10 \quad 9 \quad 8 \quad 7 \quad 6 \quad 5 \quad 4 \quad 3 \quad 2$$

  has several length-four decreasing subsequences, but no length-four increasing subsequence.
- A sequence that is either increasing or decreasing is called **monotone**.
- Our claim is that every sequence of ten distinct integers must contain a monotone, length-four subsequence.

Theorem of Erdős and Szekeres

Let n be a positive integer. Every sequence of $n^2 + 1$ distinct integers must contain a monotone subsequence of length $n + 1$.

Proof of the Theorem of Erdős and Szekeres: Labeling

- Let n be a positive integer. Suppose there is a sequence S of n^2+1 distinct integers that does not contain a monotone subsequence of length $n+1$, i.e., all monotone subsequences of S have length at most n.
  Let x be an element of the sequence S. Label x with a pair of integers (u_x, d_x), where:
  - The integer u_x is the length of a longest increasing subsequence of S that starts at x.
  - The integer d_x is the length of a longest decreasing subsequence of S that starts at x.

  For example, the sequence 1 9 10 8 3 7 5 2 6 4 would be labeled as follows:

1	9	10	8	3	7	5	2	6	4
(4,1)	(2,5)	(1,5)	(1,4)	(3,2)	(1,3)	(2,2)	(2,1)	(1,2)	(1,1)

Proof of the Theorem of Erdős and Szekeres: Pigeonholing

- Note that:
  - Because there are no monotone subsequences of length $n+1$ (or longer), the labels on the sequence S use only the integers 1 through n. Hence, we use at most n^2 labels.
  - Two distinct elements of the sequence cannot have the same label. Let x and y be distinct elements, with x appearing before y, having labels (u_x, d_x) and (u_y, d_y). Because the numbers on the list are distinct, either $x < y$ or $x > y$.
    - If $x < y$, then $u_x > u_y$: There is an increasing subsequence of length u_y starting at y. If we insert x at the beginning of this subsequence, we get an increasing subsequence of length $u_y + 1$. Thus $u_x \geq u_y + 1$, or, equivalently, $u_x > u_y$. So x and y have different labels.
    - Similarly, if $x > y$, then we have $d_x > d_y$. So again we conclude that x and y have different labels.
- Now, there are only n^2 different labels, and S has $n^2 + 1$ elements. By the Pigeonhole Principle, two of the elements must have the same label. This contradicts the second observation that no two elements can have the same label.

Bijections and Infinities

- Pigeonhole Principle: If $|A| > |B|$, there can be no one-to-one function $f : A \to B$. If $|A| < |B|$, there can be no onto function $f : A \to B$.
- So, if $f : A \to B$ is both one-to-one and onto, then $|A| = |B|$.
- Even though, these assertions are meaningful only if A and B are finite sets, it is possible to find bijections between infinite sets.
  - Example: The function $f : \mathbb{N} \to \mathbb{Z}$, with
    $$f(n) = \begin{cases} -n/2, & \text{if } n \text{ is even} \\ (n+1)/2, & \text{if } n \text{ is odd} \end{cases}$$
    is a bijection from $\mathbb{N}$ to $\mathbb{Z}$.

n	0	1	2	3	4	5	6	7	8	9
$f(n)$	0	1	-1	2	-2	3	-3	4	-4	5

  - Since there is a bijection from $\mathbb{N}$ to $\mathbb{Z}$, it makes sense to write $|\mathbb{N}| = |\mathbb{Z}|$. This means that $\mathbb{N}$ and $\mathbb{Z}$ are "just as infinite"! This may seem counterintuitive because $\mathbb{Z}$ ought to be "twice as infinite" as $\mathbb{N}$.

Cantor's Theorem

- Is it possible for two infinite sets not to have the same "size"?
- We define two sets as having the **same size** provided there is a bijection between them. In this sense, $\mathbb{N}$ and $\mathbb{Z}$ have the same size.
- Do all infinite sets have the same size? The answer is no!

Cantor's Theorem

Let A be a set. If $f : A \to 2^A$, then f is not onto.

- Let A be a set and let $f : A \to 2^A$. To show that f is not onto, we must find a $B \in 2^A$ (i.e., $B \subseteq A$), such that there is no $a \in A$ with $f(a) = B$. In other words, B is a set that f "misses."
  Let $B = \{x \in A : x \notin f(x)\}$. Suppose, there is an $a \in A$, such that $f(a) = B$. Is $a \in B$?
  - If $a \in B$, then, since $B = f(a)$, we have $a \in f(a) = B$. So, by definition of B, $a \notin B$, a contradiction!
  - If $a \notin B = f(a)$, then, by definition of B, $a \in B$, a contradiction!

  Both $a \in B$ and $a \notin B$ lead to contradictions. So, f is not onto.

Aleph Naught $\aleph_0$

- Example: Let $A = \{1, 2, 3\}$. Let $f : A \to 2^A$ be given by

a	$f(a)$	$a \in f(a)$?
1	$\{1, 2\}$	yes
2	$\{3\}$	no
3	$\emptyset$	no

  Now $B = \{x \in A : x \notin f(x)\}$. We have $B = \{2, 3\}$. Notice that there is no $a \in A$ with $f(a) = B$.
- The implication of Cantor's Theorem is that $|\mathbb{Z}| \neq |2^{\mathbb{Z}}|$. Therefore, in the sense we are exploring, $2^{\mathbb{Z}}$ is more infinite than $\mathbb{Z}$.
- Cantor proved that the smallest infinite sets have the same size as $\mathbb{N}$.
- The size of $\mathbb{N}$ is the smallest infinite cardinal $\aleph_0$ (aleph naught).

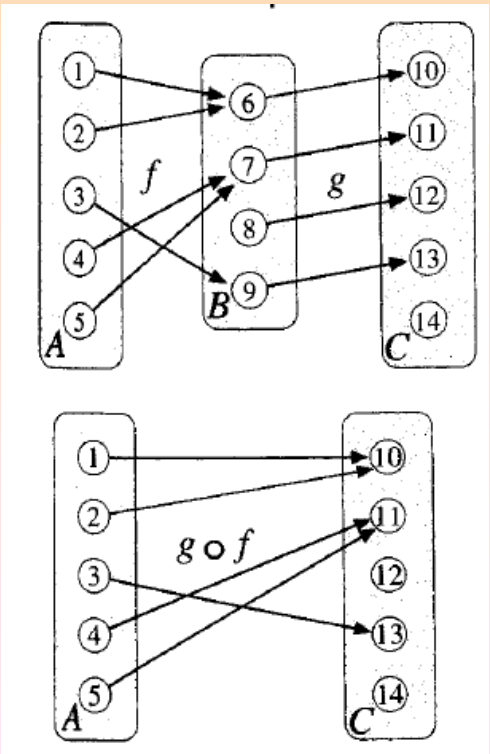
Subsection 3

Composition

Composition of Functions

Definition of Composition

Let A, B and C be sets and let $f : A \to B$ and $g : B \to C$. Then the function $g \circ f$ is a function from A to C defined by $(g \circ f)(a) = g[f(a)]$, where $a \in A$. The function $g \circ f$ is called the **composition of f and g**.



- Example: Let $A = \{1, 2, 3, 4, 5\}$, $B = \{6, 7, 8, 9\}$, and $C = \{10, 11, 12, 13, 14\}$. Let $f : A \to B$ and $g : B \to C$ be defined by $f = \{(1, 6), (2, 6), (3, 9), (4, 7), (5, 7)\}$, and $g = \{(6, 10), (7, 11), (8, 12), (9, 13)\}$. Then $(g \circ f)$ is the function $(g \circ f) = \{(1, 10), (2, 10), (3, 13), (4, 11), (5, 11)\}$.

Another Example and Some Remarks

- Let $f : \mathbb{Z} \to \mathbb{Z}$ be $f(x) = x^2 + 1$ and $g : \mathbb{Z} \to \mathbb{Z}$ be $g(x) = 2x - 3$.
  - What is $(g \circ f)(4)$?
    We calculate
    $(g \circ f)(4) = g[f(4)] = g(4^2 + 1) = g(17) = 2 \cdot 17 - 3 = 31.$
  - In general,
    $(g \circ f)(x) = g[f(x)] = g(x^2+1) = 2(x^2+1)-3 = 2x^2+2-3 = 2x^2-1.$
- The notation $g \circ f$ means that we do first f and then g.
  - The domain of $g \circ f$ is the same as the domain of f
    $\text{dom}(g \circ f) = \text{dom} f$.
  - In order for $g \circ f$ to make sense, every output of f must be an acceptable input to g. Properly said, we need $\text{im} f \subseteq \text{dom} g$. The requirements $f : A \to B$ and $g : B \to C$ ensure that the functions fit together when we form $g \circ f$.

Commutativity Does Not Hold

- Let $A = \{1, 2, 3, 4, 5\}$ and $f : A \to A$ and $g : A \to A$ be defined by

$$\begin{aligned} f &= \{(1,1),(2,1),(3,1),(4,1),(5,1)\} \\ g &= \{(1,5),(2,4),(3,3),(4,2),(5,1)\}. \end{aligned}$$

  Then:

$$\begin{aligned} g \circ f &= \{(1,5),(2,5),(3,5),(4,5),(5,5)\} \\ f \circ g &= \{(1,1),(2,1),(3,1),(4,1),(5,1)\}. \end{aligned}$$

  Thus, $g \circ f \neq f \circ g$.

- Recall the functions f and g from $\mathbb{Z}$ to $\mathbb{Z}$, given by $f(x) = x^2 + 1$ and $g(x) = 2x - 3$.
  For these, we have $(g \circ f)(4) = g[f(4)] = g(17) = 31$ and $(f \circ g)(4) = f[g(4)] = f(5) = 26$. Therefore, $g \circ f \neq f \circ g$.
  More generally,
  $(g \circ f)(x) = g[f(x)] = g[x^2 + 1] = 2[x^2 + 1] - 3 = 2x^2 - 1$ and
  $(f \circ g)(x) = f[g(x)] = f[2x - 3] = (2x - 3)^2 + 1 = 4x^2 - 12x + 10$.
  Therefore, $g \circ f \neq f \circ g$.

Associativity

Proposition (Associativity of Composition)

Let A, B, C and D be sets and let $f : A \to B$, $g : B \to C$ and $h : C \to D$. Then $h \circ (g \circ f) = (h \circ g) \circ f$.

- Let f and g be functions. To prove $f = g$:
  - Prove that $\text{dom} f = \text{dom} g$;
  - Prove that for every x in the common domain, $f(x) = g(x)$.
- To show $h \circ (g \circ f) = (h \circ g) \circ f$:
  - Check that the domains of $h \circ (g \circ f)$ and $(h \circ g) \circ f$ are the same. Since $\text{dom}(g \circ f) = \text{dom} f$, we have $\text{dom}[h \circ (g \circ f)] = \text{dom}(g \circ f) = \text{dom} f = A$ and $\text{dom}[(h \circ g) \circ f] = \text{dom} f = A$. So both functions have domain A.
  - Check that for any $a \in A$, the two functions produce the same value. Compute $[h \circ (g \circ f)](a) = h[(g \circ f)(a)] = h[g[f(a)]]$ and $[(h \circ g) \circ f](a) = (h \circ g)[f(a)] = h[g[f(a)]]$. Hence $h \circ (g \circ f) = (h \circ g) \circ f$.

Identity Functions

- The integer 1 is the identity element for multiplication, and $\emptyset$ is the identity element for union.
- What serves as an identity element for composition? There is no single identity element.

Definition of Identity Functions

Let A be a set. The **identity function on** A is the function id_A whose domain is A, and for all $a \in A$, $\mathrm{id}_A(a) = a$. I.e., $\mathrm{id}_A = \{(a, a) : a \in A\}$.

Proposition

Let A and B be sets. Let $f : A \to B$. Then $f \circ \mathrm{id}_A = \mathrm{id}_B \circ f = f$.

- To show that the functions $f \circ \mathrm{id}_A$ and f are the same:
  - $\mathrm{dom}(f \circ \mathrm{id}_A) = \mathrm{dom}\ \mathrm{id}_A = A = \mathrm{dom} f$.
  - For all $a \in A$, $(f \circ \mathrm{id}_A)(a) = f(\mathrm{id}_A(a)) = f(a)$ so $f \circ \mathrm{id}_A$ and f give the same value for all $a \in A$.
- The argument that $\mathrm{id}_B \circ f = f$ is similar.

Composing With Inverses

- Just as multiplying a rational number by its reciprocal gives 1, composing a function with its inverse gives an identity function.

Proposition (Composition with Inverse Functions)

Let A and B be sets and suppose $f : A \to B$ is one-to-one and onto. Then $f \circ f^{-1} = \mathrm{id}_B$ and $f^{-1} \circ f = \mathrm{id}_A$.

- Let us show $f \circ f^{-1} = \mathrm{id}_B$:
  - $\mathrm{dom}(f \circ f^{-1}) = \mathrm{dom} f^{-1} = B = \mathrm{dom}\ \mathrm{id}_B$.
  - Let $b \in B$. Since f is one-to-one and onto, there exists unique $a \in A$, such that $(a, b) \in f$. Then $(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b = \mathrm{id}_B(b)$.

  Therefore, $f \circ f^{-1} = \mathrm{id}_B$.
- A similar argument shows that $f \circ f^{-1} = \mathrm{id}_B$.

Subsection 4

Permutations

Permutations and the Symmetric Group S_n

Definition of Permutations

Let A be a set. A **permutation on** A is a bijection from A to itself.

- Example: Let $A = \{1, 2, 3, 4, 5\}$ and let $f : A \to A$ be

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

  Since f is a one-to-one and onto function (i.e., a bijection) from A to A, it is a permutation. Because f is a bijection, the list $(f(1), f(2), f(3), f(4), f(5)) = (2, 4, 1, 3, 5)$ is simply a reordering of $(1, 2, 3, 4, 5)$.
- It is customary to use lowercase Greek letters (especially π, σ and τ) to stand for permutations.
- The set of all permutations on $\{1, 2, \ldots, n\}$ has a special notation:

The Symmetric Group S_n

The set of all permutations on the set $\{1, 2, \ldots, n\}$ is denoted S_n. S_n is called the **symmetric group on** n **elements**.

Properties of S_n

- The identity function $\mathrm{id}_{\{1,2,\ldots,n\}}$ is a permutation and therefore in S_n. We usually denote the identity function by ι.

Proposition

There are $n!$ permutations in S_n. The set S_n satisfies:

- $\forall \pi, \sigma \in S_n, \pi \circ \sigma \in S_n$;
- $\forall \pi, \sigma, \tau \in S_n, \pi \circ (\sigma \circ \tau) = (\pi \circ \sigma) \circ \tau$;
- $\forall \pi \in S_n, \pi \circ \iota = \iota \circ \pi = \pi$;
- $\forall \pi \in S_n, \pi^{-1} \in S_n$ and $\pi \circ \pi^{-1} = \pi^{-1} \circ \pi = \iota$;

- We are missing only the proof of the first property in the list!
  - If $i, j \in \{1, 2, \ldots, n\}$, then $(\pi \circ \sigma)(i) = (\pi \circ \sigma)(j) \Rightarrow \pi(\sigma(i)) = \pi(\sigma(j)) \overset{\text{one-to-one}}{\Rightarrow} \sigma(i) = \sigma(j) \overset{\text{one-to-one}}{\Rightarrow} i = j$. So $\pi \circ \sigma$ is one-to-one.
  - If $k \in \{1, 2, \ldots, n\}$, since π is onto, there exists $j \in \{1, 2, \ldots, n\}$, such that $\pi(j) = k$. Thus, since σ is onto, there exists $i \in \{1, 2, \ldots, n\}$, such that $\sigma(i) = j$. Now $(\pi \circ \sigma)(i) = \pi(\sigma(i)) = \pi(j) = k$. So $\pi \circ \sigma$ is also onto.

Cycle Notation

- Considered the following permutation in S_5: $\pi = \{(1,2),(2,4),(3,1),(4,3),(5,5)\}$.
- There are some alternative ways of expressing permutations in S_n. We can write a $2 \times n$ array of integers: The top row contains the integers 1 through n in their usual order; the bottom row contains $\pi(1)$ through $\pi(n)$: $\pi = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{bmatrix}$
- The top row is not necessary! We could express the permutation π simply by reporting the bottom row: $\pi = [2,4,1,3,5]$.
- Another notation for expressing permutations is known as **cycle notation**: For $\pi = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{bmatrix}$ the cycle notation is $\pi = (1,2,4,3)(5)$. The two lists $(1,2,4,3)$ and (5), are called **cycles**. The cycle $(1,2,4,3)$ means that $1 \mapsto 2 \mapsto 4 \mapsto 3 \mapsto 1$. So each number k is followed by $\pi(k)$ and, finally, we "return to the start".

Writing a Permutation in Cycle Notation

- Let $\pi = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 5 & 6 & 3 & 8 & 1 & 4 & 9 \end{bmatrix}$. Express π in cycle notation.

- Note that $\pi(1) = 2, \pi(2) = 7$ and $\pi(7) = 1$. So $\pi = (1, 2, 7) \ldots$.
- The first element we have not considered is 3. Restarting from 3, we have $\pi(3) = 5$ and $\pi(5) = 3$, so the next cycle is $(3, 5)$. So far we have $\pi = (1, 2, 7)(3, 5) \ldots$.
- The next element we have yet to consider is 4. We have $\pi(4) = 6, \pi(6) = 8$ and $\pi(8) = 4$ to complete the cycle. So far we have $\pi = (1, 2, 7)(3, 5)(4, 6, 8) \ldots$.
- Finally, we have $\pi(9) = 9$, so the last cycle is just (9).
- The permutation π in cycle notation is $\pi = (1, 2, 7)(3, 5)(4, 6, 8)(9)$.

The Cycle Representation

Theorem (Existence and Uniqueness of the Cycle Representation)

Every permutation of a finite set can be expressed as a collection of pairwise disjoint cycles. Furthermore, this representation is unique up to rearranging the cycles and the cyclic order of the elements within cycles.

- Let $\pi \in S_n$. Consider the sequence $1, \pi(1), (\pi \circ \pi)(1), (\pi \circ \pi \circ \pi)(1), \ldots$ which we can rewrite $1, \pi(1), \pi^{(2)}(1), \pi^{(3)}(1), \ldots$. This is a sequence of integers in $\{1, 2, \ldots, n\}$, so eventually it must repeat itself. Suppose the first repeat is at $\pi^{(k)}(1)$.
  - We show $\pi^{(k)}(1) = 1$.
    Suppose, for the sake of contradiction, that $\pi^{(k)}(1) \neq 1$. In this case, we have $\pi^{(k)}(1) = \pi^{(j)}(1)$, where $0 < j < k$. Because this is the first repeat, we have $\pi^{(k-1)}(1) \neq \pi^{(j-1)}(1)$. Since π is one-to-one, applying π to both sides yields $\pi^{(k)}(1) \neq \pi^{(j)}(1)$ a contradiction!
- The cycle starting at element 1 might not include all the elements of $\{1, 2, \ldots, n\}$. In this case, we can restart with an "unused" element and start building a new cycle.

Existence of the Cycle Representation (Cont'd)

- Is it possible that a new cycle "runs into" an existing cycle?
  - We show that, if the element s is not an element of the cycle $(t, \pi(t), \pi^{(2)}(t), \ldots)$, it is not possible that $\pi^{(k)}(s)$ is an element of this cycle for any $k \geq 0$.
    Suppose that s is not an element of the cycle $(t, \pi(t), \pi^{(2)}(t), \ldots)$. To show that $\pi^{(k)}(s)$ is not an element of this cycle for any $k \geq 0$, we use the smallest counterexample method. Let k be the smallest natural number for which $\pi^{(k)}(s)$ is in $(t, \pi(t), \pi^{(2)}(t), \ldots)$, say $\pi^{(k)}(s) = \pi^{(j)}(t)$.
    - By hypothesis, since s not in $(t, \pi(t), \pi^{(2)}(t), \ldots)$, $k > 0$.
    - Consider $\pi^{(k-1)}(s)$. By the smallest property of k, $\pi^{(k-1)}(s)$ is not in $(t, \pi(t), \pi^{(2)}(t), \ldots)$, so $\pi^{(k-1)}(s) \neq \pi^{(j-1)}(t)$. Since π is one-to-one, $\pi^{(k)}(s) \neq \pi^{(j)}(t)$, a contradiction!
- Therefore we can write π as a collection of pairwise disjoint cycles; i.e., such that no two of the cycles have a common element.

Uniqueness of the Cycle Representation

- Is it possible to write the same permutation as a collection of disjoint cycles in two different ways?
- We may write, for example,

$$\pi = (1,2,7)(3,5)(4,6,8)(9) = (5,3)(6,8,4)(9)(7,1,2).$$

- However, on closer inspection, the two representations of π have the same cycles.
- There is only one way to write π as a collection of disjoint cycles.
  - Suppose, for the sake of contradiction, that we had two ways to write π. Then an element, say element 1, would be listed in one cycle in the first representation and in a different cycle in the second representation. However, if we consider the sequence, $1, \pi(1), \pi^{(2)}(1), \pi^{(3)}(1), \ldots$ we see that the two different cycles would predict two different sequences. This is impossible since the sequence is solely dependent on π and not on the notation in which π is written.

Inverting Permutations

- How do we compute the inverse of a permutation expressed in cycle notation?
  If π maps $a \mapsto b$, then π^{-1} maps $b \mapsto a$. Thus, if $(a, b, c, \ldots)$ is a cycle of π, then $(\ldots, c, b, a)$ is a cycle of π^{-1}.
- Example: Let $\pi = (1, 2, 7, 9, 8)(5, 6, 3)(4) \in S_9$. Calculate π^{-1}.

  $\pi^{-1} = (8, 9, 7, 2, 1)(3, 6, 5)(4)$.

  Check that for $k \in \{1, 2, \ldots, 9\}$, if $\pi(k) = j$ (j follows k in a cycle in π), then $\pi^{-1}(j) = k$ (k follows j in a cycle of π^{-1}).

Composing Permutations

- We compute the composition of two permutations in cycle notation.
- Example: Let $\pi, \sigma \in S_9$ be given by $\pi = (1,3,5)(4,6)(2,7,8,9)$, and $\sigma = (1,4,7,9)(2,3)(5)(6,8)$. We compute $\pi \circ \sigma$.
  To do this, we calculate $(\pi \circ \sigma)(k)$ for all $k \in \{1,2,\ldots,9\}$.
  We begin with $(\pi \circ \sigma)(1)$. $(\pi \circ \sigma)(1) = \pi(4) = 6$, and we can write $\pi \circ \sigma = (1,6,\ldots$. To continue the cycle, we calculate $(\pi \circ \sigma)(6)$. $\pi \circ \sigma$ maps $6 \mapsto 9$. Now we have $\pi \circ \sigma = (1,6,9,\ldots$. Next we compute $(\pi \circ \sigma)(9) = \pi(1) = 3$, so $\pi \circ \sigma = (1,6,9,3,\ldots$. Continuing in this fashion, we get $1 \mapsto 6 \mapsto 9 \mapsto 3 \mapsto 7 \mapsto 2 \mapsto 5 \mapsto 1$ and we have completed a cycle! Thus $(1,6,9,3,7,2,5)$ is a cycle of $\pi \circ \sigma$. Notice that 4 is not on this cycle, so we start over computing $(\pi \circ \sigma)(4)$. We find $4 \mapsto 8$. The second cycle in $\pi \circ \sigma$ begins $(4,8,\ldots$. Now we calculate $(\pi \circ \sigma)(8) = 4$, so the entire cycle is simply $(4,8)$. The two cycles $(1,6,9,3,7,2,5)$ and $(4,8)$ exhaust all the elements of $\{1,2,\ldots,9\}$, and so we are finished. We have found $\pi \circ \sigma = (1,6,9,3,7,2,5)(4,8)$.

Transpositions

- The simplest permutation is the identity permutation ι; it satisfies $\iota(x) = x$ for every x in its domain.
- The next simplest type of permutation is called a transposition; transpositions map almost all elements to themselves, except that they exchange one pair of elements, as, e.g., in $\tau = (1)(2)(3,6)(4)(5)(7)(8)(9) \in S_9$.

Definition of Transpositions

A permutation $\tau \in S_n$ is called a **transposition** provided

- there exist $i, j \in \{1, 2, \ldots, n\}$ with $i \neq j$ so that $\tau(i) = j$ and $\tau(j) = i$;
- for all $k \in \{1, 2, \ldots, n\}$ with $k \neq i$ and $k \neq j$, we have $\tau(k) = k$.

- When a transposition is written in cycle notation, the vast majority of the cycles are singletons. So it is more convenient not to write out all these 1-cycles and to write just $\tau = (3,6)$ instead of $\tau = (1)(2)(3,6)(4)(5)(7)(8)(9)$.

Converting a Cycle Into Composition of Transpositions

- Trick for converting a cycle into a composition of transpositions:
- Example: Let $\pi = (1, 2, 3, 4, 5)$. Write π as the composition of transpositions.
  $(1, 2, 3, 4, 5) = (1, 5) \circ (1, 4) \circ (1, 3) \circ (1, 2)$.
- Let $\pi = (1, 2, 3, 4, 5)(6, 7, 8)(9)(10, 11)$. Write π as the composition of transpositions.
  $\pi = [(1, 5) \circ (1, 4) \circ (1, 3) \circ (1, 2)] \circ [(6, 8) \circ (6, 7)] \circ (10, 11)$.

Theorem (Transposition Representation)

Let π be any permutation on a finite set. Then π can be expressed as the composition of transpositions defined on that set.

- Let π be any permutation. Write π as a composition of disjoint cycles. Using the technique above, rewrite each of its cycles as a composition of transpositions. The cycles are disjoint, so there is no effect of one cycle on another. Thus, we can string together the transpositions for the various cycles into one long composition of cycles.

Uniqueness of Parity

- The decomposition of a permutation into transpositions is not unique. For example, we can write

$$\begin{aligned}(1,2,3,4) &= (1,4)\circ(1,3)\circ(1,2)\\ &= (1,2)\circ(2,3)\circ(3,4)\\ &= (1,2)\circ(1,4)\circ(2,3)\circ(1,4)\circ(3,4).\end{aligned}$$

  These ways of writing $(1,2,3,4)$ are not rearrangements of one another. They do not even have the same length.

- However, they do have something in common! All three compositions consist of an odd number of transpositions.

Inversions in a Permutation I

Definition of Inversion in a Permutation

Let $\pi \in S_n$ and let $i, j \in \{1, 2, \ldots, n\}$ with $i < j$. The pair i, j is called an **inversion in** π if $\pi(i) > \pi(j)$.

- We calculate the number of inversions in a transposition $(a, b) \in S_n$. Let us assume $a < b$ so we can write this as $(a, b) =$

$$\begin{bmatrix} 1 & 2 & \cdots & a-1 & a & a+1 & \cdots & b-1 & b & b+1 & \cdots & n \\ 1 & 2 & \cdots & a-1 & b & a+1 & \cdots & b-1 & a & b+1 & \cdots & n \end{bmatrix}.$$

The only inversions possible are those that involve a or b. We count three types of inversions:

  - Those involving only a: Element a has advanced from column a to column b. In so doing, it has skipped past elements $a+1, a+2, \ldots, b-1$ and creates inversions with those elements. It is still in its proper order with respect to all other columns. The number of inversions of this sort is $(b-1) - (a+1) + 1 = b - a - 1$.

Inversions in a Permutation II

- We continue counting inversions in the transposition $(a, b) = \begin{bmatrix} 1 & 2 & \cdots & a-1 & a & a+1 & \cdots & b-1 & b & b+1 & \cdots & n \\ 1 & 2 & \cdots & a-1 & b & a+1 & \cdots & b-1 & a & b+1 & \cdots & n \end{bmatrix}$.
  - Those involving only b: Element b has retreated from column b to column a. In so doing, it has ducked under elements $a+1, a+2, \ldots, b-1$ and creates inversions with those elements. It is still in its proper order with respect to all other columns. The number of inversions of this sort is, again, $(b-1)-(a+1)+1 = b-a-1$.
  - Those involving both a and b: This is just one inversion.

  The total number of inversions is $2(b-a-1)+1$, an odd number.
- Note the number of inversions involving a but not b equals the number of inversions involving b but not a. Further, all these inversions involve the elements appearing between a and b.

Evenness of the Identity

Lemma

If the identity permutation is written as a composition of transpositions, then that composition must use an even number of transpositions. That is, if $\iota = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_a$, where the τs are transpositions, then a must be even.

- Write ι as a composition of transpositions: $\iota = \tau_a \circ \tau_{a-1} \circ \cdots \circ \tau_2 \circ \tau_1$. Our goal is to prove that a is even. We apply the transpositions τ_i one at a time.
  - We first apply τ_1. The resulting number of inversions is now odd.
  - We show that as we apply each τ_i, the number of inversions changes by an odd amount.

  The number of inversions at the start and at the end is zero. Since each transposition increases or decreases the number of inversions by an odd amount, the number of transpositions must be even.

Evenness of the Identity (Cont'd)

- We wrote $\iota = \tau_a \circ \tau_{a-1} \circ \cdots \circ \tau_2 \circ \tau_1$.
- Suppose $\tau_k = (a, b)$ and $\tau_{k-1} \circ \cdots \circ \tau_1 = \begin{bmatrix} \cdots & i & \cdots & m & \cdots & j & \cdots \\ \cdots & a & \cdots & x & \cdots & b & \cdots \end{bmatrix}$. When we apply $\tau_k = (a, b)$, the effect is $\tau_k \circ \tau_{k-1} \circ \cdots \circ \tau_1 = \begin{bmatrix} \cdots & i & \cdots & m & \cdots & j & \cdots \\ \cdots & b & \cdots & x & \cdots & a & \cdots \end{bmatrix}$. The only change is that a and b are exchanged in the bottom row. What has happened to the number of inversions?
  - For a pair of columns including neither column i nor column j, there is no change.
  - Columns to the left of column i and columns to the right of column j are unaffected by the interchange of a and b; these elements do not change their order with respect to these outer columns. Therefore we only need to pay attention to columns between columns i and j.

Evenness of the Identity (Cont'd)

- Let's say that column m is between i and j, and the entry in column m is x. When we exchange a and b, the bottom row changes from $[\cdots a \cdots x \cdots b \cdots]$ to $[\cdots b \cdots x \cdots a \cdots]$. Consider cases depending on x's size compared to a and b:
  - If $x < a$ and $x < b$, then there is no change in the number of inversions involving x and a or b. Before applying τ_k we had a and x inverted, but x and b were in natural order. After applying τ_k we have x and b inverted, but x and a are in their natural order.
  - If $x > a$ and $x > b$, then there is no change in the number of inversions involving x and a or b; the argument is similar.
  - If $a < x < b$, then upon switching a and b, we gain two inversions involving a and x and involving b and x.
  - If $a > x > b$, then upon switching a and b, we lose two inversions.

  In every case, the number of inversions either stays the same or changes by two. The exchange of a and b either increases the number of inversions by one (if $a < b$) or decreases the number of inversions by one (if $a > b$). The cumulative effect is an odd change.

Parity Theorem

Theorem (Uniqueness of Parity)

Let $\pi \in S_n$ be decomposed into transpositions as $\pi = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_a$ and $\pi = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_b$. Then a and b have the same parity, i.e., they are both odd or both even.

- Let π be a permutation decomposed into transpositions as $\pi = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_a$ and $\pi = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_b$.
  We can write $\pi^{-1} = \sigma_b \circ \sigma_{b-1} \circ \cdots \circ \sigma_2 \circ \sigma_1$. So
  $\iota = \pi \circ \pi^{-1} = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_a \circ \sigma_b \circ \sigma_{b-1} \circ \cdots \circ \sigma_2 \circ \sigma_1$.
  This is a decomposition of ι into $a + b$ transpositions. Hence, by the previous lemma, $a + b$ is even, and so a and b have the same parity.

Even and Odd Permutations

Definition of Even and Odd Permutations

Let π be a permutation on a finite set.

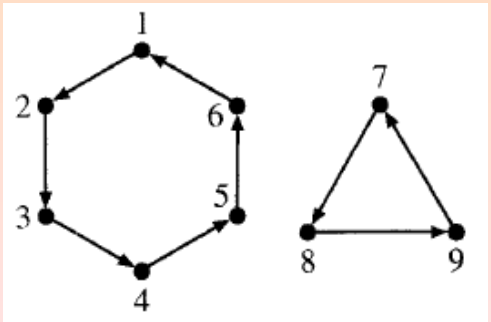
- We call π **even** provided it can be written as the composition of an even number of transpositions.
- Otherwise, it can be written as the composition of an odd number of transpositions, in which case we call π **odd**.

- The **sign** of a permutation is ± 1 depending on whether the permutation is odd or even.
  The sign of π is:

$$\text{sgn}\pi = \begin{cases} +1, & \text{if } \pi \text{ is even} \\ -1, & \text{if } \pi \text{ is odd} \end{cases}.$$

Permutation Diagrams

- We may draw a picture of a permutation:
- Given $\pi \in S_n$, we make a figure in which
  - the numbers $1, 2, \ldots, n$ are represented by points;
  - if $\pi(a) = b$, we draw an arrow from a to b.
- In case $\pi(a) = a$, we draw a looping arrow from a to itself.
- Example: If $\pi = (1, 2, 3, 4, 5, 6)(7, 8, 9)$, then



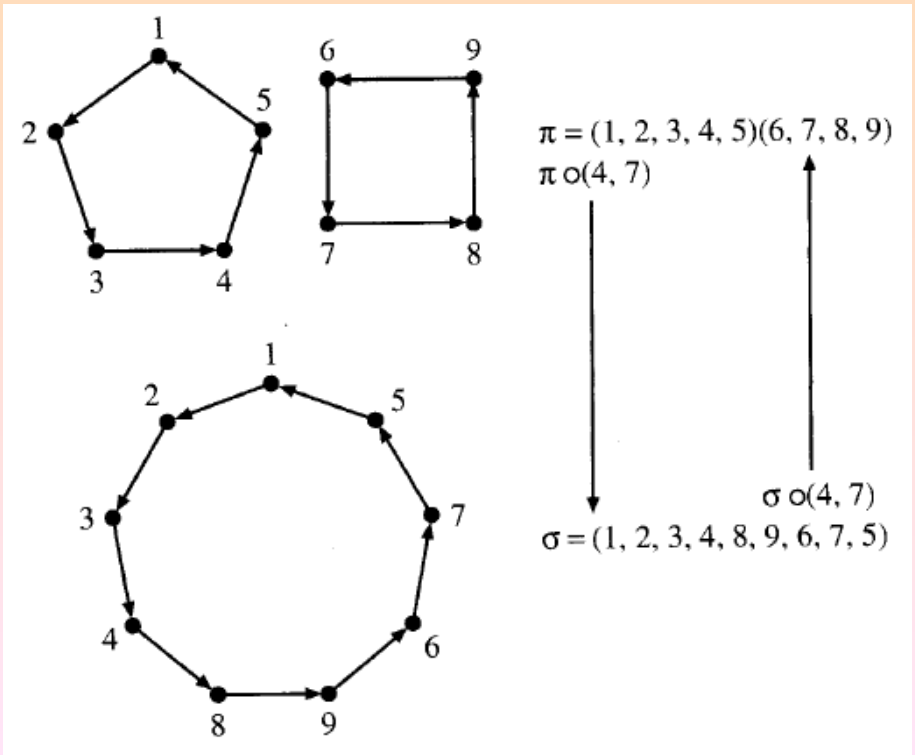
- Each cycle of π corresponds precisely to a closed path in the diagram.
- Suppose we compose a permutation π with a transposition τ. What is the effect on the diagram of π?

Composing With a Transposition

- Suppose $\pi, \tau \in S_n$ and $\tau = (a, b)$ where $a \neq b$ and $a, b \in \{1, 2, \ldots, n\}$.
- When we express π as disjoint cycles, cycles that contain neither a nor b are the same in π and $\pi \circ \tau$.
- The only cycles that are affected are ones that contain a or b.
  - If a and b are in the same cycle, then π is of the form $\pi = (p, a, q, \ldots, s, b, t, \ldots, z)(\cdots)$. Then $\pi \circ (a, b)$ will be of the form $\pi \circ (a, b) = (p, a, q, \ldots, s, b, t, \ldots, z)(\cdots) \circ (a, b) = (p, a, t, \ldots, z)(q, \ldots, s, b)(\cdots)$. In other words, the cycle containing a and b in π is split into two cycles in $\pi \circ (a, b)$: one containing a and the other containing b.
  - If a and b are in different cycles, the opposite effect occurs. In this case, π is of the form $\pi = (p, a, q, \ldots)(s, b, t, \ldots)(\cdots)$ and so $\pi \circ (a, b)$ has the form $\pi \circ (a, b) = (p, a, q, \ldots)(s, b, t, \ldots)(\cdots) \circ (a, b) = (p, a, t, \ldots, s, b, q, \ldots)(\cdots)$. The cycles containing a and b in π are merged into a single cycle in $\pi \circ (a, b)$.

An Example

- Suppose $\pi = (1,2,3,4,5)(6,7,8,9)$ and let $\sigma = \pi \circ (4,7)$. Then, $\sigma = (1,2,3,4,8,9,6,7,5)$. Because 4 and 7 are in separate cycles of π, they are in a common cycle of $\pi \circ (4,7)$.
- Conversely, 4 and 7 are in the same cycle of σ but are split into separate cycles in $\sigma \circ (4,7)$.



Connections With the Parity Theorem

Proposition

Let n be a positive integer and $\pi, \tau \in S_n$, and suppose τ is a transposition. Then the number of cycles in the disjoint cycle representations of π and $\pi \circ \tau$ differ by exactly one.

- Suppose $\pi \in S_n$ and $\pi = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_a$, where the τs are transpositions. We will show that

$$a = n - c(\pi) \pmod 2, \tag{1}$$

  where $c(\pi)$ is the number of cycles in the unique disjoint cycle representation of π.
- So the parity of the number of transpositions in Equation (1) equals the parity of $n - c(\pi)$.
- This implies that two different decompositions of π into transpositions will both have an even or both have an odd number of terms.

Expression for the Sign of a Permutation

- Consider the sequence $\iota, \tau_1, \tau_1 \circ \tau_2, \tau_1 \circ \tau_2 \circ \tau_3, \ldots, \pi$. Each term is formed from the previous by appending the appropriate τ_j. We calculate $n - c(\bullet)$ for each of these permutations

σ	ι	τ_1	$\tau_1 \circ \tau_2$	$\tau_1 \circ \tau_2 \circ \tau_3$	$\cdots$	π
$n - c(\sigma)$	0	1	1 ± 1	$1 \pm 1 \pm 1$	$\cdots$	$\underbrace{1 \pm 1 \pm \cdots \pm 1}_{a \text{ terms}}$

Note that the parity of the expression $1 \pm 1 \pm 1 \pm \cdots \pm 1$ (with a terms) is exactly the same as the parity of a, and the result follows.

Corollary

Let n be a positive integer and $\pi \in S_n$. Then $\operatorname{sgn}\pi = (-1)^{n-c(\pi)}$.

Subsection 5

Symmetry

Introduction

- We close by briefly studying the concept of symmetry.
- What does it mean to say that "an object is symmetric"?
- The word symmetry typically refers to geometric figures.
- An informal definition of symmetry of a figure is as a motion that, when applied to an object, results in a figure that looks exactly the same as the original.
- Example: If we rotate a square sitting on the plane counterclockwise about its center through an angle of 90°, the resulting figure is exactly the same as the original. However, if we rotate the square through an angle of, say, 30°, the resulting figure is not the same as the original. Therefore, a 90° rotation is a symmetry of the square, but a 30° rotation is not.

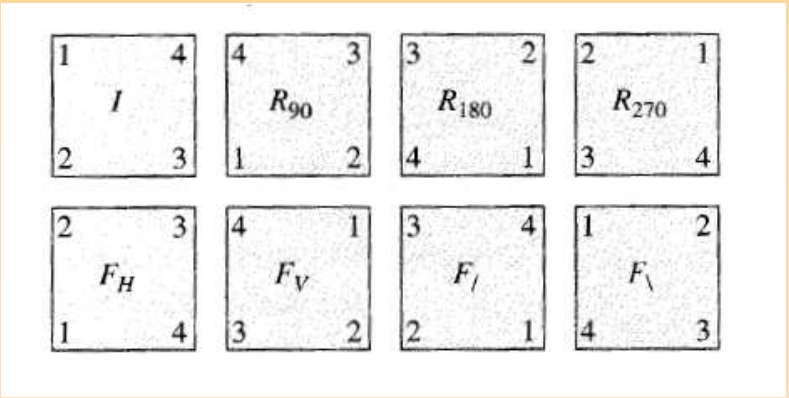
Symmetries of a Square: Rotations

- Rotating a square 90° counterclockwise through its center leaves the square unchanged.
- What are the other motions we can apply to a square that leave it unchanged?
- Write the numbers 1 through 4 in the corners of the square.
  - We call the counterclockwise rotation through 90° symmetry R_{90}.
  - We may also rotate the square counterclockwise through 180°. We call this symmetry R_{180}. We might also rotate the square clockwise through 180°, but the end result is identical with R_{180}.
  - We can rotate the square through 270° and leave the image unchanged. We call this symmetry R_{270}.
  - Finally, we can rotate the square through 360° and the result is unchanged. Instead of R_{360}, we call this symmetry I, for **identity**.
- So far we have found four symmetries: I, R_{90}, R_{180} and R_{270}. Are there more?

Symmetries of a Square: Reflections or Flips

- We can pick the square up, flip it over, and set it back down in the plane.
  - We can flip the square over along a horizontal axis. We call this symmetry F_H for "flip-horizontal."
  - We can also flip the square over along its vertical axis. We call that motion F_V, or "flip-vertical."
  - We can also hold the square by two opposite corners and flip it over along its diagonal. If we rotate through the upper-right to lower-left corner axis, we call this symmetry $F_/$ or "flip along the / diagonal."
  - We can also rotate along the upper-left to lower-right corner axis and flip over along the \ diagonal. We call this symmetry $F_\backslash$.
- The eight symmetries found thus far are $I, R_{90}, R_{180}, R_{270}, F_H, F_V, F_/$, and $F_\backslash$.

The Eight Symmetries of the Square

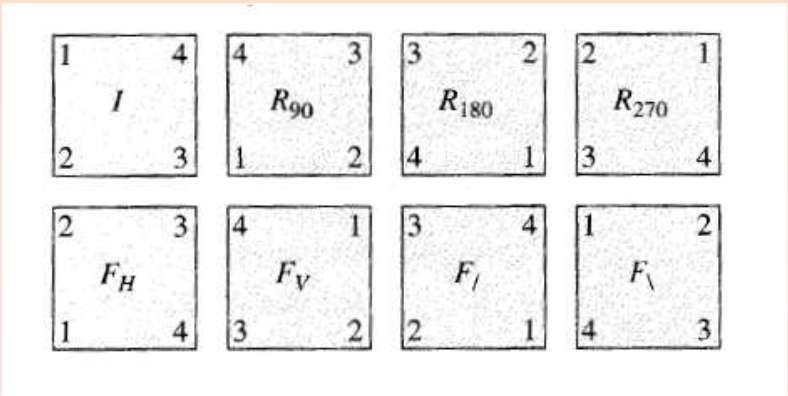


- Are there any duplications? The answer is no. We observe that no two of the squares are labeled the same.
- Are there any other symmetries? The answer to this question is also no. Where could the corner labeled 1 possibly go?
  - It might end up in the northeast, northwest, southeast, or southwest.
  - Once we have decided where corner 1 goes, there are only two choices for corner 2, since it must end up next to corner 1.
  - Once we have placed corners 1 and 2, the remaining corners are forced into position.

Therefore, there are $4 \times 2 = 8$ choices, so we have found all the symmetries.

Symmetries as Permutations

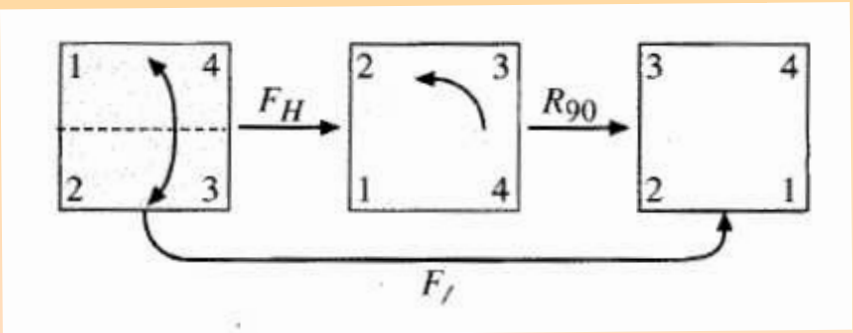
- The symmetry R_{90} can be expressed as $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}$. The first column means that label 1 moves to position 2, the second column means that label 2 moves to position 3, and so on.
- Since it is a permutation, we can express it in cycle form as $(1, 2, 3, 4)$.
- All eight symmetries of the square can be expressed in this notation.



Name	1 2 3 4	Cycle Form
I	1 2 3 4	$(1)(2)(3)(4)$
R_{90}	2 3 4 1	$(1, 2, 3, 4)$
R_{180}	3 1 4 2	$(1, 3)(2, 4)$
R_{270}	4 1 2 3	$(1, 4, 3, 2)$
F_H	2 1 4 3	$(1, 2)(3, 4)$
F_V	4 3 2 1	$(1, 4)(2, 3)$
$F_/$	3 2 1 4	$(1, 3)(2)(4)$
$F_\backslash$	1 4 3 2	$(1)(2, 4)(3)$

Combining Symmetries

- What happens if we first flip the square horizontally and then rotate it through 90°?



  The net effect is a flip along the / diagonal, (i.e., $F_/$). This is written $R_{90} \circ F_H = F_/$ ($\circ$ denoting "symmetry combination").
- Recall that in $g \circ f$, the function f is applied first and then g.
- Since the symmetries of the square can be thought of as relabeling permutations of its corners, we get

$$R_{90} \circ F_H = (1,2,3,4) \circ (1,2)(3,4) = (1,3)(2)(4) = F_/.$$

- Even though the first $\circ$ stands for combining symmetries, and the second $\circ$ is permutation composition, the calculation gives the correct answer for the symmetries.

How Combination Works

- We first do F_H, which we can express as $\pi = (1,2)(3,4)$. The effect is to take whatever is in position 1 (label 1) to position 2. Then $\sigma = (1,2,3,4)$ takes whatever is in position 2 (label 2) to position 3. So the net effect is $1 \mapsto 2 \mapsto 3$. The other corners work the same way.
- We can make an 8×8 chart showing the combined effect of each pair of symmetries:

$\circ$	I	R_{90}	R_{180}	R_{210}	F_H	F_V	$F_/$	$F_\backslash$
I	I	R_{90}	R_{180}	R_{270}	F_H	F_V	$F_/$	$F_\backslash$
R_{90}	R_{90}	R_{180}	R_{270}	I	$F_/$	$F_\backslash$	F_V	F_H
R_{180}	R_{180}	R_{270}	I	R_{90}	F_V	F_H	$F_\backslash$	$F_/$
R_{270}	R_{270}	I	R_{90}	R_{180}	$F_\backslash$	$F_/$	F_H	F_V
F_H	F_H	$F_\backslash$	F_V	$F_/$	I	R_{180}	R_{270}	R_{90}
F_V	F_V	$F_/$	F_H	$F_\backslash$	R_{180}	I	R_{90}	R_{270}
$F_/$	$F_/$	F_H	$F_\backslash$	F_V	R_{90}	R_{270}	I	R_{180}
$F_\backslash$	$F_\backslash$	F_V	$F_/$	F_H	R_{270}	R_{90}	R_{180}	I

Properties of Combination

- The operation $\circ$ is not commutative. For instance, $R_{90} \circ F_H = F_/$ but $F_H \circ R_{90} = F_\backslash$.
- Element I is an identity element for $\circ$.
- Every element has an inverse. For example, $R_{90}^{-1} = R_{270}$ because $R_{90} \circ R_{270} = R_{270} \circ R_{90} = I$. Most of the elements are their own inverse.
- The operation $\circ$ is associative. We noted that we can replace symmetries by permutations and then interpret $\circ$ as composition.
- In summary, the operation $\circ$ is associative, has an identity element, and every symmetry has an inverse.
- The operation of composition on the set of all permutations of n elements, S_n, also exhibits these same properties.

Isometry

- A geometric figure, e.g., a square, is a set of points in the plane $\mathbb{R}^2$.
- Example: The following set is a square:

$$S = \{(x, y) \in \mathbb{R}^2 : -1 \leq x \leq 1, -1 \leq y \leq 1\}.$$

- The **distance** between points (a, b) and (c, d) is

$$\text{dist}[(a, b), (c, d)] = \sqrt{(a - c)^2 + (b - d)^2}.$$

where $\text{dist}[(a, b), (c, d)]$ stands for the distance between the points (a, b) and (c, d).

Definition of Isometry

Let $f : \mathbb{R}^2 \to \mathbb{R}^2$. We call f an **isometry** provided

$$\forall (a, b), (c, d) \in \mathbb{R}^2, \text{dist}[(a, b), (c, d)] = \text{dist}[f(a, b), f(c, d)].$$

- A synonym for isometry is a **distance-preserving function**.

Symmetry

- Let $X \subseteq \mathbb{R}^2$ (i.e., X is a geometric figure).
- If $f : \mathbb{R}^2 \to \mathbb{R}^2$, writing $f(X)$ is nonsense because X is a set of points and the domain of f is the set of points in the plane.
- However, we define $f(X)$ to mean

$$f(X) = \{f(a, b) : (a, b) \in X\}.$$

So, $f(X)$ is the set we obtain by evaluating f at all the points in X.

Definition of Symmetry

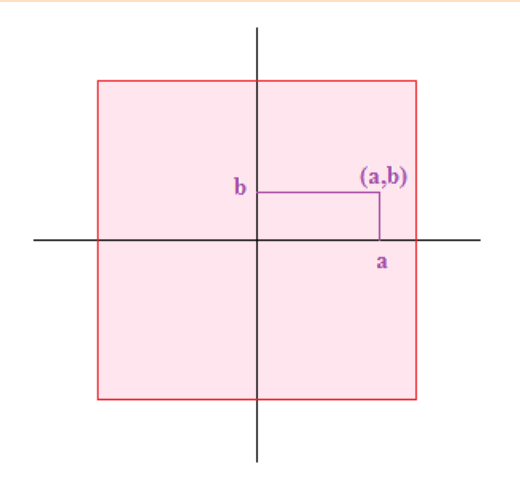
Let $X \subseteq \mathbb{R}^2$. A **symmetry** of X is an isometry $f : \mathbb{R}^2 \to \mathbb{R}^2$ such that $f(X) = X$.

Symmetries of the Square Revisited

- Consider again the square

$$S = \{(x, y) \in \mathbb{R}^2 : -1 \leq x \leq 1, -1 \leq y \leq 1\}.$$

The symmetries of S are



$$I(a, b) = (a, b) \qquad F_H(a, b) = (a, -b)$$
$$R_{90}(a, b) = (-b, a) \qquad F_V(a, b) = (-a, b)$$
$$R_{180}(a, b) = (-a, -b) \qquad F_{/}(a, b) = (b, a)$$
$$R_{270}(a, b) = (b, -a) \qquad F_{\backslash}(a, b) = (-b, -a).$$

- Even though we focused on geometric figures in the plane, all these ideas can be extended to three-dimensional space and beyond.