# Queen's University
# School of Computing

# CISC 203: Discrete Mathematics for Computing II
# Module 6: Functions
# Fall 2021

This module corresponds to the following sections from your textbook:

24. Functions
25. The Pigeonhole Principle
26. Composition
27. Permutations

## 1 Functions

**Definition 1** (Function)**.** A relation $f : A \longrightarrow B$ is called a function if $(a, b) \in f$ and $(a, c) \in f$ implies $b = c$.

Intuitively, a function is a "machine" that transforms one quantity into another, but each input quantity can not have more than one output quantity.

**Example 2.** Let

$$f = \{(1, 2), (2, 3), (3, 1), (4, 7)\} \text{ and } g = \{(1, 2), (1, 3), (4, 7)\}.$$

The relation $f$ is a function but the relation $g$ is not a function because $(1, 2), (1, 3) \in g$ and $2 \neq 3$.

If $f$ is a function whose output value is $y$ when the input is $x$, we write $f(x) = y$. We say that $f$ maps $x$ to $y$.

For example, we can can express function $f(x) = x^2$ on the integers as a set of ordered pairs, as

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

We can also express it in set-builder notation as

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

As another example, the absolute value function *abs* takes an integer $x$ as input and returns $x$ if $x$ is positive and returns $-x$ if $x$ is negative, i.e.,

$$f(x) = abs(x) = |x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0. \end{cases}$$

Similarly, *abs* can also be expressed as a set of ordered pairs, or in set-builder notation as

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

**Definition 3** (Domain and Image)**.** The **domain** of a relation or function $g$ is the set of all the **first elements** of the ordered pairs in $g$. We denote this as

$$\text{dom } g = \{a \in A : \exists b \in B, (a, b) \in g\},$$

or alternatively,

$$\text{dom } g = \{a \in A : g(a) \text{ is defined}\}.$$

The **image** of a relation or function $g$ is the set of all the **second elements** of the ordered pairs in $g$. We denote this as

$$\text{im } g = \{b \in B : \exists a \in A, (a, b) \in g\},$$

or alternatively,

$$\text{im } g = \{b \in B : b = g(a) \text{ for some } a\}.$$

**Definition 4** ($f : A \longrightarrow B$)**.** A function from set $A$ to set $B$, denoted

$$f : A \longrightarrow B,$$

is a rule that assigns to each element $a \in A$ a unique element $f(a) \in B$.

The domain of $f$ is the set $A$, i.e., dom $f = A$. In other words, for every element $a \in A$ there is a pair $(a, b)$ in $f$.

The image of $f$ is a subset of $B$, i.e., im $f \subseteq B$.

In the *abs* function above, the argument of the function is an integer and the value is a non-negative integer so we may write $abs : \mathbb{Z} \longrightarrow \mathbb{N}$.

**Definition 5** (One-to-one, Onto, Bijection)**.** Consider a function $f : A \longrightarrow B$.

- The function $f$ is called **one-to-one** (or **injective**) if whenever $(a_1, b), (a_2, b) \in f,$ we must have $a_1 = a_2$. In other words, if $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$.
- The function $f$ is called **onto** $B$ (or **surjective**) if for every $b \in B$, there exists an $a \in A$ such that $f(a) = b$.
- The function $f$ is a **bijection** if it is both one-to-one and onto.

**Exercise**

Let $A = \{1, 2\}$ and $B = \{3, 4\}$. Write down all functions $f : A \longrightarrow B$. Indicate which are one-to-one and which are onto $B$.

To prove that a function is one-to-one, it must be shown that when $f(a_1) = f(a_2)$, we have $a_1 = a_2$. This can also be done by contrapositive or by contradiction (see Proof Template 20, p. 172).

To prove that a function $f : A \longrightarrow B$ is onto $B$, show that for every element $b \in B$ there must be an element $a \in A$ such that $f(a) = b$. Alternatively, show that the set $B$ is equal to im $f$ (see Proof Template 21, p. 173).

**Example 6.** Let $A$ be the set of even integers and $B$ be the set of odd integers. The function $f : A \longrightarrow B$ defined by $f(x) = x + 1$ is a bijection.

*Proof.* We must prove that $f$ is both one-to-one and onto.

To show that $f$ is one-to-one, suppose $f(a_1) = f(a_2)$, where $a_1$ and $a_2$ are even integers:

$$f(a_1) = f(a_2) \quad \Longrightarrow \quad a_1 + 1 = a_2 + 1 \quad \Longrightarrow \quad a_1 = a_2$$

So, $f$ is one-to-one.

To show that $f$ is onto $B$, let $b$ be any element from $B$ (i.e., an odd integer). By definition, $b = 2k + 1$ for some integer $k$. Let $a = 2k$; since $a$ is clearly even, we have $a \in A$. Then, $f(a) = a + 1 = 2k + 1 = b$. So, $f$ is onto.

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

**Example 7.** The function $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $f(x) = x^2$ is not one-to-one and not onto $\mathbb{Z}$.

*Proof.* $f(3) = f(-3) = 9$, but $3 \neq -3$, so $f$ is not one-to-one.

It is not onto $\mathbb{Z}$ either, since $f(x)$ can never be a negative integer, so $\operatorname{im} f \neq \mathbb{Z}$. □

**Example 8.** The function $f : \mathbb{R} \longrightarrow \mathbb{Z}$ defined by the floor function $f(x) = \lfloor x \rfloor$ is onto $\mathbb{Z}$ but not one-to-one.

*Proof.* To show that $f$ is onto $\mathbb{Z}$, let $b$ be any integer. We take $a = b$, which is clearly in $\mathbb{R}$. Then, $f(a) = \lfloor a \rfloor = \lfloor b \rfloor = b$. So, $f$ is onto.

$f(3.1) = f(3.3) = 3$, but $3.1 \neq 3.3$, so $f$ is not one-to-one. □

**Exercise**

Show that the function $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $f(x) = 2x$ is one-to-one but not onto.

### 1.1 Inverse functions

Any relation $R \subseteq A \times B$ has a unique inverse relation $R^{-1} \subseteq B \times A$. However, the inverse relation of a function $f$ need not be a function, as shown in the following counterexample.

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

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

so

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

$f^{-1}$ is not a function from $B$ to $A$, for two reasons:

1. $f^{-1}$ is not a function, since $(7, 1)$ and $(7, 4)$ are in $f^{-1}$. This violates Definition 1.
2. $\operatorname{dom} f^{-1} \neq B$. This violates Definition 4. See Example 24.12 in the textbook for an illustration.

**Theorem 10.** *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.*

*Note that if $f$ is one-to-one, but not onto, the inverse relation $f^{-1}$ is still a function, but $\operatorname{dom} f^{-1}$ (which is equal to $\operatorname{im} f$) will be a proper subset of $B$ (and thus $f^{-1}$ would not be a function from $B$ to $A$, by Definition 4).*

## 2 The Pigeonhole Principle

The **Pigeonhole Principle** states that: If $n$ pigeons are put into $m$ holes, where $n > m$, then at least one hole will contain more than one pigeon. To illustrate, suppose there are nine holes in a pigeon coop, and ten pigeons fly to the coop to roost. If each of the ten pigeons is in a hole, then it must be the case that at least one hole contains more than one pigeon.

The following two propositions follow from the Pigeonhole Principle.

**Proposition 11.** *For a function $f : A \longrightarrow B$ where $A$ and $B$ are finite sets:*

*i. if $|A| > |B|$, then $f$ is not one-to-one; and* *ii. if $|A| < |B|$, then $f$ is not onto.*

We illustrate this with two examples.

**Example 12.** Let $A = \{1, 2, 3\}$ and $B = \{4, 5\}$. Since $|A| > |B|$, there is no function $f : A \longrightarrow B$ that is one-to-one.

Let $A = \{1, 2\}$ and $B = \{3, 4, 5\}$. Since $|B| > |A|$, there is no function $f : A \longrightarrow B$ that is onto.

The next proposition follows from the above proposition.

**Proposition 13.** *Let $A$ and $B$ be finite sets and let $f : A \longrightarrow B$. If $f$ is a bijection, then $|A| = |B|$.*

**Exercise**

Let $A = \{1, 2, 3\}$ and $B = \{4, 5\}$. Give a function $f : A \longrightarrow B$ that is onto.

Let $A = \{1, 2\}$ and $B = \{3, 4, 5\}$. Give a function $f : A \longrightarrow B$ that is one-to-one.

The following is a generalized version of the Pigeonhole Principle.

**Proposition 14.** *If $n$ elements are partitioned into $m$ subsets, then at least one subset must contain $\lceil n/m \rceil$ or more elements.*

**Proof.** Suppose we have $n$ elements partitioned into $m$ subsets. For the sake of contradiction, suppose that no subset contains more than $\lceil n/m \rceil - 1$ elements. Then the total number of elements is at most

$$m\left(\left\lceil \frac{n}{m} \right\rceil - 1\right) < m\left(\left(\frac{n}{m} + 1\right) - 1\right) = n.$$

Thus, we must have fewer than $n$ elements. However, we assumed we had exactly $n$ elements. Therefore, our assumption was incorrect and at least one subset must contain at least $\lceil n/m \rceil$ elements. □

**Example 15.** In the 2017–2018 academic year, there were 11 783 students enrolled in the Faculty of Arts and Science at Queen's University. Assume that each of these students was born in the same four-year period of 1996–1999. The given four-year period consisted of 1 461 days. Therefore, by the pigeonhole principle, at least $\lceil 11\,783/1\,461 \rceil = 9$ students in the Faculty of Arts and Science were born on the same day.

Note that Proposition 11 and Proposition 13 are meaningful only for finite sets. For example, consider the set $A$ of all positive integers $\{1, 2, 3, \ldots\}$ and the set $B$ of all nonnegative integers $\{0, 1, 2, 3, \ldots\}$. But the function $f : A \longrightarrow B$ defined by $f(x) = x - 1$ is a bijection, even though $A$ is a proper subset of $B$. Refer to p. 180 of your textbook for another bijection from $\mathbb{N}$ to $\mathbb{Z}$.

# 3 Composition

The *composition* of functions $f : A \longrightarrow B$ and $g : B \longrightarrow C$ is the function $g \circ f : A \to C$ defined by

$$(g \circ f)(a) = g(f(a)) \text{ for every } a \in A.$$

Note that the composition is defined only if the image of $f$ equals the domain of $g$.

When dealing with a function composition $g \circ f$ it is important to remember that the function $f$ is applied first, and then apply function $g$ to the resulting value.

**Example 16.** Let $A = \{1, 2, 3, 4, 5\}$, $B = \{6, 7, 8, 9\}$, and $C = \{10, 11, 12, 13, 14\}$. Let $f : A \longrightarrow B$ and $g : B \longrightarrow C$ 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

$$(g \circ f) = \{(1, 10), (2, 10), (3, 13), (4, 11), (5, 11)\}.$$

For example, we can calculate $(g \circ f)(3)$ as follows.

$$(g \circ f)(3) = g(f(3)) = g(9) = 13.$$

Which means $(3, 13) \in g \circ f$.

**Example 17.** Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ by $f(x) = x^2 + 1$ and $g : \mathbb{Z} \longrightarrow \mathbb{Z}$ by $g(x) = 2x - 3$.

For example, we can calculate $(g \circ f)(3)$ as follows.

$$(g \circ f)(3) = g(f(3)) = g(3^2 + 1) = g(10) = 2 \times 10 - 3 = 17.$$

In general,

$$\begin{aligned}(g \circ f)(x) &= g(f(x))\\ &= g(x^2 + 1)\\ &= 2(x^2 + 1) - 3\\ &= 2x^2 + 2 - 3\\ &= 2x^2 - 1\end{aligned}$$

Note that you may verify the value of $(g \circ f)(3)$ by plugging 3 into the general expression for $(g \circ f)(x)$. We also note that the composition of functions is not commutative. For this example, we see that $(g \circ f)(3) \neq (f \circ g)(3)$:

$$(f \circ g)(3) = f(g(3)) = f(2 \times 3 - 3) = f(3) = 3^2 + 1 = 10.$$

To prove that two functions $f$ and $g$ are equal, we must show that:

1. The domain of $f$ equals the domain of $g$; and
2. For every $x$ in their common domain, $f(x) = g(x)$.

Refer to Proof Template 22 on p. 185 of your textbook.

So in the previous example, $g \circ f \neq f \circ g$ since we showed that $(g \circ f)(3) \neq (f \circ g)(3)$ (which violates the second condition above).

The composition of functions is associative. For $f : A \longrightarrow B$, $g : B \longrightarrow C$ and $h : C \longrightarrow D$ we have

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

This is proved in Proposition 26.6 (p. 185) of your textbook.

**Definition 18** (Identity function)**.** The *identity function* on a set $A$, $\mathrm{id}_A : A \to A$, is defined as $\mathrm{id}_A(a) = a$ for all $a \in A$.

The identity function is a bijection. For example, the identify function on $\mathbb{N}$, denoted as a set of ordered pairs, is

$$\mathrm{id}_{\mathbb{N}} = \{(0, 0), (1, 1), (2, 2), (3, 3), \ldots\}.$$

**Example 19.** Let $A$ and $B$ be sets, and let $f : A \longrightarrow B$. We will prove that $f \circ \mathrm{id}_A = \mathrm{id}_B \circ f = f$, using Proof Template 22.

*Proof.* The first condition of Proof Template 22 is satisfied, since we have:

$$\operatorname{dom}(f \circ \mathrm{id}_A) = \operatorname{dom}(\mathrm{id}_A) = A = \operatorname{dom}(f)$$

and

$$\operatorname{dom}(\mathrm{id}_B \circ f) = \operatorname{dom}(f)$$

The second condition of Proof Template 22 is satisfied, since we have:

$$(f \circ \mathrm{id}_A)(a) = f(\mathrm{id}_A(a)) = f(a)$$

and

$$(\mathrm{id}_B \circ f)(a) = \mathrm{id}_B(f(a)) = f(a).$$

So, we have shown that $f \circ \mathrm{id}_A = \mathrm{id}_B \circ f = f$. □

**Proposition 20.** *Let $A$ and $B$ be sets and suppose $f : A \longrightarrow B$ is one-to-one and onto. Then,*

$$f^{-1} \circ f = \mathrm{id}_A$$

*and*

$$f \circ f^{-1} = \mathrm{id}_B,$$

*where $f^{-1}$ is the inverse of $f$.*

**Exercise**

Prove the above proposition, using the same technique (i.e., with Proof Template 22).

# 4 Permutations

**Definition 21** (Permutation)**.** Given a set $A$, a permutation of $A$ is a bijective function $\pi : A \to A$.

A permutation is a function that maps elements of a set $A$ to elements of the same set $A$. In other words, if our informal definition of a permutation is an arrangement of elements, then the permutation $\pi$ itself is what performs the rearranging of elements.

**Example 22.** Suppose we have a set $A = \{1, 2, 3, 4, 5, 6\}$. Let $\pi : A \longrightarrow A$ be a function given by:

$$\begin{aligned} \pi(1) &= 3; & \pi(4) &= 2; \\ \pi(2) &= 4; & \pi(5) &= 1; \\ \pi(3) &= 5; & \pi(6) &= 6. \end{aligned}$$

We see that $\pi$ is a bijection from $A$ to $A$.

We can more compactly represent the permutation $\pi$ from the previous example using certain notations. The **two-line notation** uses a two-line matrix; the first line lists the elements of the set $A$, and the second line lists the permuted elements $\pi(1)$ through $\pi(6)$. Thus,

$$\pi = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{bmatrix}.$$

What happens if we compose $\pi$ with itself? Let's trace what happens to the element 1. We are going to apply $\pi$ twice: The first application maps 1 to 3, and the second application maps 3 to 5. If we apply $\pi$ a third time, 5 is mapped back to 1. Treating $\pi$ as a function, we see that $\pi(1) = 3$, $(\pi \circ \pi)(1) = 5$, and

$(\pi \circ \pi \circ \pi)(1) = 1$. We can write this **cycle** as $(1, 3, 5)$. Repeating the same process by tracing the elements 2 and 6 gives us the two cycles $(2, 4)$ and $(6)$, respectively. So in **cycle notation**, we can write

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

In this notation, each set of parentheses represents a cycle, where the first element is mapped to the second element, the second element is mapped to the third element, and so on, and the last element is mapped back to the first element. Since the element 6 is always mapped to 6, we can leave that cycle out, giving us

$$\pi = (1, 3, 5)(2, 4).$$

Note that we can write $\pi \circ \pi$ as $\pi^2$, $\pi \circ \pi \circ \pi$ as $\pi^3$, and so on.

Composing permutations is just like composing other functions. If $\pi$ and $\sigma$ are permutations on a set, we can write $\pi \circ \sigma$ to represent the result of applying $\sigma$ (as a function) and then applying $\pi$.

**Example 23.** Let

$$\pi = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{bmatrix} \text{ and } \sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}.$$

We calculate $\pi \circ \sigma$ as follows:

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

The result is in fact another permutation. This follows from the fact that the composition of two bijections will always be a bijection. We can create a diagram to visualize the composition of these two permutations, as follows.

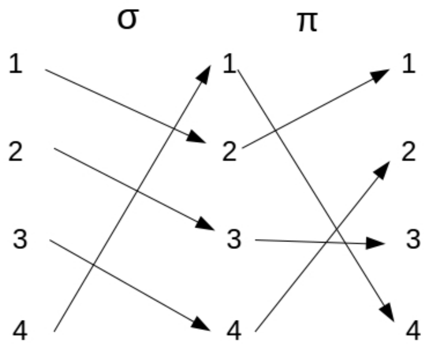

Figure 1: Visual representation of the composition of $\pi$ and $\sigma$ in Example 23.

We can also just think of the operation of a permutation as "turns $x$ into $y$", so we can interpret $\pi \circ \sigma(3)$ as "$\sigma$ turns 3 into 4, then $\pi$ turns 4 into 2".

**Exercise**

Write $\pi$, $\sigma$, $\pi \circ \sigma$, $\sigma \circ \pi$ from the previous example in cycle notation.

**Theorem 24.** *Every permutation can be expressed as a collection of pairwise disjoint cycles. Furthermore, this representation is unique up to rearranging the cycles and cyclic order of the elements within cycles.*

**Definition 25** **($S_n$).** 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—we will revisit this when we cover Groups later in the course.

**Example 26.** Here, we list all permutations on the set $\{1, 2\}$ and on the set $\{1, 2, 3\}$.

$$S_2 = \left\{ \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \right\} = \{(1)(2), (1, 2)\}$$

$$\begin{aligned} S_3 &= \left\{ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \right\} \\ &= \{(1)(2)(3), (1, 2)(3), (1, 3)(2), (1)(2, 3), (1, 2, 3), (1, 3, 2)\} \end{aligned}$$

Note that in $S_2$, $(1)(2) = \text{id}_{\{1,2\}}$ is the identity function on the set $\{1, 2\}$. In $S_3$, $(1)(2)(3) = \text{id}_{\{1,2,3\}}$ is the identity function on the set $\{1, 2, 3\}$. For the identity function, we typically simplify the cycle notation to $(1)$, so we can write $\text{id}_{\{1,2\}} = (1)$ and $\text{id}_{\{1,2,3\}} = (1)$ without any confusion.

We denote the identity function with the Greek letter $\iota$. In fact we almost always use Greek letters to name permutations: $\pi$, $\sigma$, and $\tau$ are among the favourites.

**Example 27.** Let $\pi \in S_9$ be given by

$$\pi = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 6 & 8 & 9 \\ 1 & 2 & 6 & 4 & 5 & 3 & 7 & 8 & 9 \end{bmatrix}.$$

In cycle notation, $\pi = (1)(2)(3, 6)(4)(5)(7)(8)(9) = (3, 6)$. We write $\iota \in S_9$ as $\iota = (1)$.

**Proposition 28.** *There are $n!$ permutations in $S_n$. The set $S_n$ satisfies the following properties.*

1. *Closure: If $\pi \in S_n$ and $\sigma \in S_n$, then $\pi \circ \sigma \in S_n$.*
2. *Associativity: If $\pi \in S_n$ and $\sigma \in S_n$ and $\tau \in S_n$, then $\pi \circ (\sigma \circ \tau) = (\pi \circ \sigma) \circ \tau$.*
3. *Identity element: There is a permutation $\iota$ such that $\pi \circ \iota = \iota \circ \pi = \pi, \forall \pi \in S_n$.*
4. *Inverse: If $\pi \in S_n$, then $\pi^{-1} \in S_n$ and $\pi \circ \pi^{-1} = \pi^{-1} \circ \pi = \iota$.*

Each of the above properties follow from the definition of permutations and the properties of functions.

Property 1 says that the composition of two permutations is another permutation. This sounds trivial but it is our first look at a very important concept: **closure**. When we apply an operation to two elements of a set and **always** get another element of the same set, we say that set is **closed** under that operation.

Not all sets are closed under all operations. For example, $\mathbb{N}$ is not closed under the operation of subtraction (for instance, $3 \in \mathbb{N}$ and $4 \in \mathbb{N}$, but $3 - 4 = -1$, and $-1 \notin \mathbb{N}$). However, $\mathbb{N}$ **is** closed under addition and multiplication. This concept is vital to us as computer scientists because we frequently work with strongly typed programming languages, where each variable has a specific type that cannot change. If we are dealing with integer variables, we need to be sure the operations we perform will only produce integer values.

Property 2 is called the associative property. It says that if we are composing a sequence of permutations we can group them with parentheses in different ways without changing the result.

Property 3 asserts that the identity permutation $\iota$ can be composed with any permutation without changing it. Once again, we can draw a parallel to other sets and operations. For example, in the set $\mathbb{N}$ and the operation of multiplication, we know that for all $x \in \mathbb{N}$, $x \times 1 = 1 \times x = x$.

Property 4 asserts that every permutation has an inverse. This property is also true for some sets and operations but not all. For example, in the set $\mathbb{Z}$ and the operation of addition, the identity element is 0 and every element has an inverse (for instance, the inverse of 7 is -7). However in the set $\mathbb{N}$ and the operation of addition, the identity element is still 0 but the non-zero values do not have inverses (for instance there is no integer $x \in \mathbb{N}$ such that $8 + x = 0$).

Property 4 is particularly important when we use permutations in cryptography—there's not much point encoding information with a permutation if there is not some other permutation that will do the decoding.

Side note: A set and an operation that satisfy these four properties are called a **group**. Group theory is one of the most important branches of mathematics, with applications in communications, theoretical physics, applied physics, biology, chemistry, robotics and many other fields. We will learn about groups in Chapter 8.

Note that there is a property possessed by many operations that is not true of the composition of permutations: commutativity. Commutativity holds when we can switch the left-to-right order of the operands without changing the result. For example, when we are adding integers, we know that $x + y = y + x$ and the same is true for multiplication. Not all operations are commutative. For example, subtraction is not commutative: $x - y \neq y - x$ except when $x = y$. **Composition of permutations is not commutative.** In general, $\pi \circ \sigma \neq \sigma \circ \pi$ (but they can be equal in some special cases).

**Example 29.** Given permutations $\pi$ and $\sigma$ in $S_n$, we can always find a permutation $\alpha$ such that $\pi \circ \alpha = \sigma$:

$$\begin{aligned}
\pi \circ \alpha &= \sigma \\
\pi^{-1} \circ (\pi \circ \alpha) &= \pi^{-1} \circ \sigma \\
(\pi^{-1} \circ \pi) \circ \alpha &= \pi^{-1} \circ \sigma \\
\iota \circ \alpha &= \pi^{-1} \circ \sigma \\
\alpha &= \pi^{-1} \circ \sigma
\end{aligned}$$

It's easy to check that this is correct: If we take $\pi \circ \alpha$ and replace $\alpha$ by $\pi^{-1} \circ \sigma$, we get:

$$\begin{aligned}
\pi \circ \alpha &= \pi \circ (\pi^{-1} \circ \sigma) \\
&= (\pi \circ \pi^{-1}) \circ \sigma \\
&= \iota \circ \sigma \\
&= \sigma
\end{aligned}$$

But this means that to find $\alpha$ we need to know $\pi^{-1}$. We will see that there are at least two simple ways to calculate $\pi^{-1}$ when we are given $\pi$.

## 4.1 Computing the Inverse of a Permutation

Suppose we have a permutation $\pi$ and we need to compute $\pi^{-1}$. We could do it from the standard matrix representation.

**Example 30.** Consider

$$\pi = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 5 & 2 & 7 & 3 & 6 \end{bmatrix}.$$

To compute $\pi^{-1}$, we can see that $\pi(1) = 4$, so we know that $\pi^{-1}(4) = 1$. Similarly, we see that $\pi(4) = 2$, so we know that $\pi^{-1}(2) = 4$, and so on. Then, we obtain

$$\pi^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 6 & 1 & 3 & 7 & 5 \end{bmatrix}.$$

But with the permutation expressed in cycle notation, computing $\pi^{-1}$ is simpler: we just reverse each cycle. The cycle notation of $\pi$ is $(1, 4, 2)(3, 5, 7, 6)$, so $\pi^{-1}$ is simply $(2, 4, 1)(6, 7, 5, 3)$.

Note that **reversing** a cycle is very different from **rotating** a cycle: if we consider the $(a, b, c, d)$, the cycle $(c, d, a, b)$ is equivalent, but the cycle $(d, c, b, a)$ is the inverse. It is a common practice to start each cycle with the lowest number within the cycle, and to order the cycles so that the initial values are in ascending order. So, we can rewrite $\pi^{-1}$ in this example as $(1, 2, 4)(3, 6, 7, 5)$.

## 4.2 Transpositions

**Definition 31** (Transposition)**.** 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 $\tau(j) = i$, and
- for all $k \in \{1, 2, \ldots, n)$ with $k \neq i$ and $k \neq j$, we have $\tau(k) = k$.

Trapositions exchange one pair of elements, and map each of the remaining elements to themselves. We have already encountered a transposition in Example 27. We now give two examples that show how to write any permutation as a composition of transpositions. Observe that there is a nice trick for converting a cycle into a composition of transpositions.

**Example 32.** Let $\pi = (1, 2, 3, 4, 5)$. We write $\pi$ as the composition of transpositions as

$$(1, 2, 3, 4, 5) = (1, 5) \circ (1, 4) \circ (1, 3) \circ (1, 2).$$

**Example 33.** Let $\pi = (1, 4, 2)(3, 5, 7, 6)$. We write $\pi$ as the composition of transpositions as

$$(1, 4, 2)(3, 5, 7, 6) = (1, 2) \circ (1, 4) \circ (3, 6) \circ (3, 7) \circ (3, 5).$$

**Exercise**

Write the permutation $\pi = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 1 & 6 & 5 & 3 & 8 & 9 & 7 \end{smallmatrix}\right]$ as (i) in cycle notation (i.e., as a composition of disjoint cycles), and (ii) as a composition of transpositions.

Note that the decomposition of a permutation into transpositions is not unique, e.g.,

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

However, note that each decomposition has an odd number of transpositions. More generally, we have the following theorem.

**Theorem 34.** *Let $\pi \in S_n$. Consider any two decompositions of $\pi$ that we denote 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 $b$ must have the same parity, i.e., they are both odd or both even.*

*Proof.* See the proof of Theorem 27.12 on p. 193 of the textbook. □

This theorem allows us to give the following definition, which we will revisit when we study groups.

**Definition 35** (Even and odd permutations)**.** Let $\pi$ be a permutation on a finite set. We call $\pi$ **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 $\pi$ **odd**.