Discrete Mathematics

Topic 04 — Relations and Functions

Lecture 04 — Function Operations

Dr Kieran Murphy

Department of Computing and Mathematics,
SETU (Waterford).
(kieran.murphy@setu.ie)

Autumn Semester, 2024

Outline

- Function Operations
- Inverse of a Function — existence conditions and derivation

Outline

Functions — Where are we ?

At this point we have:

- defined what a function is (any process that generates exactly one output for each input)
- covered fundamental concepts (source, target, domain, image),
- covered properties (injective, surjective and bijective).

we want to discuss

- function operations — constructing new functions by adding/multiplying functions* or by applying one function after another function.
- function inverse — finding function pairs that have the property that applying one after the other results in the original input.
- yet another graphical representation of functions — using 2D Cartesian graphs to represent functions.
- a library of useful functions in computing.

*These are a bigger deal in calculus than in discrete mathematics

Evaluating Functions

Before we start combining functions, I want to make sure that you are happy with evaluating a function.†

Example 1

Given the function $f : x \mapsto 2x^2 - x + 3$, evaluate

1. $f(-a)$
2. $f(2a)$
3. $f(a+h)$
4. $f(x+5)$

1. $f(-a)$

$$f(-a) = 2\left[-a\right]^2 - \left[-a\right] + 3 = 2a^2 + a + 3$$

2. $f(2a)$

$$f(2a) = 2\left[2a\right]^2 - \left[2a\right] + 3 = 8a^2 - 2a + 3$$

3. $f(a+h)$

$$f(a+h) = 2\left[a+h\right]^2 - \left[a+h\right] + 3 = 2a^2 + 4ah + 2h^2 - a - h + 3$$

4. $f(x+5)$

$$f(x+5) = 2\left[x+5\right]^2 - \left[x+5\right] + 3 = 2x^2 + 10x - x + 48$$

† Simply use an extra set of brackets to ensure correct order of operations.

Evaluating Functions

Before we start combining functions, I want to make sure that you are happy with evaluating a function.†

Example 1

Given the function $f : x \mapsto 2x^2 - x + 3$, evaluate

1. $f(-a)$
2. $f(2a)$
3. $f(a+h)$
4. $f(x+5)$

1. $f(-a)$

$$f(-a) = 2[-a]^2 - [-a] + 3 = 2a^2 + a + 3$$

2. $f(2a)$

$$f(2a) = 2[2a]^2 - [2a] + 3 = 8a^2 - 2a + 3$$

3. $f(a+h)$

$$f(a+h) = 2[a+h]^2 - [a+h] + 3 = 2a^2 + 4ah + 2h^2 - a - h + 3$$

4. $f(x+5)$

$$f(x+5) = 2[x+5]^2 - [x+5] + 3 = 2x^2 + 10x - x + 48$$

† Simply use an extra set of brackets to ensure correct order of operations.

Evaluating Functions

Before we start combining functions, I want to make sure that you are happy with evaluating a function.[†]

Example 1

Given the function $f : x \mapsto 2x^2 - x + 3$, evaluate

1. $f(-a)$
2. $f(2a)$
3. $f(a+h)$
4. $f(x+5)$

1. $f(-a)$
$$f(-a) = 2\left[-a\right]^2 - \left[-a\right] + 3 = 2a^2 + a + 3$$
2. $f(2a)$
$$f(2a) = 2\left[2a\right]^2 - \left[2a\right] + 3 = 8a^2 - 2a + 3$$
3. $f(a+h)$
$$f(a+h) = 2\left[a+h\right]^2 - \left[a+h\right] + 3 = 2a^2 + 4ah + 2h^2 - a - h + 3$$
4. $f(x+5)$
$$f(x+5) = 2\left[x+5\right]^2 - \left[x+5\right] + 3 = 2x^2 + 10x - x + 48$$

[†] Simply use an extra set of brackets to ensure correct order of operations.

Evaluating Functions

Before we start combining functions, I want to make sure that you are happy with evaluating a function.†

Example 1

Given the function $f : x \mapsto 2x^2 - x + 3$, evaluate

1. $f(-a)$
2. $f(2a)$
3. $f(a+h)$
4. $f(x+5)$

1. $f(-a)$
$$f(-a) = 2\left[-a\right]^2 - \left[-a\right] + 3 = 2a^2 + a + 3$$
2. $f(2a)$
$$f(2a) = 2\left[2a\right]^2 - \left[2a\right] + 3 = 8a^2 - 2a + 3$$
3. $f(a+h)$
$$f(a+h) = 2\left[a+h\right]^2 - \left[a+h\right] + 3 = 2a^2 + 4ah + 2h^2 - a - h + 3$$
4. $f(x+5)$
$$f(x+5) = 2\left[x+5\right]^2 - \left[x+5\right] + 3 = 2x^2 + 10x - x + 48$$

†Simply use an extra set of brackets to ensure correct order of operations.

Function Equality

Two functions are equal if they have the same domain and the same rule/mapping.

Definition 2 (Function Equality)

Let f and g be two functions. Then

$$f = g \iff \underbrace{\mathrm{Dom}(f) = \mathrm{Dom}(g)}_{\text{same domain}} \wedge \underbrace{f(x) = g(x) \quad \forall x \in \mathrm{Dom}(f)}_{\text{same rule}}$$

- Two functions that have different domains cannot be equal. For example,

$$f : \mathbb{Z} \to \mathbb{Z} : x \mapsto x^2 \qquad \text{and} \qquad g : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$$

are **not** equal even though the rule that defines them is the same.

- However, it is not uncommon for two functions to be equal even though they are defined differently. For example

$$h : \{-1, 0, 1, 2\} \to \{0, 1, 2\} : x \mapsto |x|$$

and

$$k : \{-1, 0, 1, 2\} \to \{0, 1, 2\} : x \mapsto -\frac{x^3}{3} + x^2 + \frac{x}{3}$$

appear to be very different functions. However, they are equal because, domains are equal and $h(x) = k(x)$ for all $x \in \{-1, 0, 1, 2\}$.

Function Equality

Two functions are equal if they have the same domain and the same rule/mapping.

Definition 2 (Function Equality)

Let f and g be two functions. Then

$$f = g \iff \underbrace{\mathrm{Dom}(f) = \mathrm{Dom}(g)}_{\text{same domain}} \wedge \underbrace{f(x) = g(x) \quad \forall x \in \mathrm{Dom}(f)}_{\text{same rule}}$$

- Two functions that have different domains cannot be equal. For example,

$$f : \mathbb{Z} \to \mathbb{Z} : x \mapsto x^2 \qquad \text{and} \qquad g : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$$

  are **not** equal even though the rule that defines them is the same.
- However, it is not uncommon for two functions to be equal even though they are defined differently. For example

$$h : \{-1, 0, 1, 2\} \to \{0, 1, 2\} : x \mapsto |x|$$

  and

$$k : \{-1, 0, 1, 2\} \to \{0, 1, 2\} : x \mapsto -\frac{x^3}{3} + x^2 + \frac{x}{3}$$

  appear to be very different functions. However, they are equal because, domains are equal and $h(x) = k(x)$ for all $x \in \{-1, 0, 1, 2\}$.

Function Equality

Two functions are equal if they have the same domain and the same rule/mapping.

Definition 2 (Function Equality)

Let f and g be two functions. Then

$$f = g \qquad \Longleftrightarrow \qquad \underbrace{\mathrm{Dom}(f) = \mathrm{Dom}(g)}_{\text{same domain}} \quad \wedge \quad \underbrace{f(x) = g(x) \quad \forall x \in \mathrm{Dom}(f)}_{\text{same rule}}$$

- Two functions that have different domains cannot be equal. For example,

  $$f : \mathbb{Z} \to \mathbb{Z} : x \mapsto x^2 \qquad \text{and} \qquad g : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$$

  are **not** equal even though the rule that defines them is the same.
- However, it is not uncommon for two functions to be equal even though they are defined differently. For example

  $$h : \{-1, 0, 1, 2\} \to \{0, 1, 2\} : x \mapsto |x|$$

  and

  $$k : \{-1, 0, 1, 2\} \to \{0, 1, 2\} : x \mapsto -\frac{x^3}{3} + x^2 + \frac{x}{3}$$

  appear to be very different functions. However, they are equal because, domains are equal and $h(x) = k(x)$ for all $x \in \{-1, 0, 1, 2\}$.

Function Addition/Subtraction/Multiplication/Division

I'm throwing these four operations together in the hope that you see that this is just notational convenience‡. You will cover these more formally in your *Calculus* module.

Definition 3

Given two functions $f : x \mapsto f(x)$ and $g : x \mapsto g(x)$ then (informally) the

- sum function is
$$(f + g) : x \mapsto f(x) + g(x)$$
- difference function is
$$(f - g) : x \mapsto f(x) - g(x)$$
- product function is
$$(fg) : x \mapsto f(x)g(x)$$
- quotient function is
$$(f/g) : x \mapsto f(x)/g(x) \qquad g(x) \neq 0$$

‡What programmers call "syntax sugar".

Example 4

Example 4

Let $f : x \mapsto x^4 - 16$ and $g : x \mapsto |x| - 4$ Determine

1. $(f+g)(2)$
2. $(fg)(2)$
3. $\left(\frac{f}{g}\right)(2)$
4. $\left(\frac{g}{f}\right)(2)$
5. $\left(\frac{g}{f}\right)(1)$

1. $(f+g)(2) = f(2) + g(2) = [0] + [-2] = -2$
2. $(fg)(2) = f(2)g(2) = [0] \cdot [-2] = 0$
3. $\left(\frac{f}{g}\right)(2) = \frac{f(2)}{g(2)} = \frac{0}{-2} = 0$
4. $\left(\frac{g}{f}\right)(2) = \frac{g(2)}{f(2)} = \frac{-2}{0} = \text{not allowed} \implies 2 \notin \text{Dom}(g/f)$
5. $\left(\frac{g}{f}\right)(1) = \frac{g(1)}{f(1)} = \frac{-3}{-15} = \frac{1}{5}$

Example 4

Example 4

Let $f : x \mapsto x^4 - 16$ and $g : x \mapsto |x| - 4$ Determine

1. $(f+g)(2)$
2. $(fg)(2)$
3. $\left(\frac{f}{g}\right)(2)$
4. $\left(\frac{g}{f}\right)(2)$
5. $\left(\frac{g}{f}\right)(1)$

1. $(f+g)(2) = f(2) + g(2) = [0] + [-2] = -2$
2. $(fg)(2) = f(2)g(2) = [0] \cdot [-2] = 0$
3. $\left(\frac{f}{g}\right)(2) = \frac{f(2)}{g(2)} = \frac{0}{-2} = 0$
4. $\left(\frac{g}{f}\right)(2) = \frac{g(2)}{f(2)} = \frac{-2}{0} = \text{not allowed} \implies 2 \notin \mathrm{Dom}(g/f)$
5. $\left(\frac{g}{f}\right)(1) = \frac{g(1)}{f(1)} = \frac{-3}{-15} = \frac{1}{5}$

Example 4

Example 4

Let $f : x \mapsto x^4 - 16$ and $g : x \mapsto |x| - 4$ Determine

1. $(f+g)(2)$
2. $(fg)(2)$
3. $\left(\frac{f}{g}\right)(2)$
4. $\left(\frac{g}{f}\right)(2)$
5. $\left(\frac{g}{f}\right)(1)$

1. $(f+g)(2) = f(2) + g(2) = [0] + [-2] = -2$
2. $(fg)(2) = f(2)g(2) = [0] \cdot [-2] = 0$
3. $\left(\frac{f}{g}\right)(2) = \frac{f(2)}{g(2)} = \frac{0}{-2} = 0$
4. $\left(\frac{g}{f}\right)(2) = \frac{g(2)}{f(2)} = \frac{-2}{0} = \text{not allowed} \implies 2 \notin \text{Dom}(g/f)$
5. $\left(\frac{g}{f}\right)(1) = \frac{g(1)}{f(1)} = \frac{-3}{-15} = \frac{1}{5}$

Example 4

Example 4

Let $f : x \mapsto x^4 - 16$ and $g : x \mapsto |x| - 4$ Determine

1. $(f+g)(2)$
2. $(fg)(2)$
3. $\left(\dfrac{f}{g}\right)(2)$
4. $\left(\dfrac{g}{f}\right)(2)$
5. $\left(\dfrac{g}{f}\right)(1)$

1. $(f+g)(2) = f(2) + g(2) = [0] + [-2] = -2$
2. $(fg)(2) = f(2)g(2) = [0] \cdot [-2] = 0$
3. $\left(\dfrac{f}{g}\right)(2) = \dfrac{f(2)}{g(2)} = \dfrac{0}{-2} = 0$
4. $\left(\dfrac{g}{f}\right)(2) = \dfrac{g(2)}{f(2)} = \dfrac{-2}{0} =$ not allowed $\implies 2 \notin \mathrm{Dom}(g/f)$
5. $\left(\dfrac{g}{f}\right)(1) = \dfrac{g(1)}{f(1)} = \dfrac{-3}{-15} = \frac{1}{5}$

Example 4

Example 4

Let $f : x \mapsto x^4 - 16$ and $g : x \mapsto |x| - 4$ Determine

1. $(f+g)(2)$
2. $(fg)(2)$
3. $\left(\dfrac{f}{g}\right)(2)$
4. $\left(\dfrac{g}{f}\right)(2)$
5. $\left(\dfrac{g}{f}\right)(1)$

1. $(f+g)(2) = f(2) + g(2) = [0] + [-2] = -2$
2. $(fg)(2) = f(2)g(2) = [0] \cdot [-2] = 0$
3. $\left(\dfrac{f}{g}\right)(2) = \dfrac{f(2)}{g(2)} = \dfrac{0}{-2} = 0$
4. $\left(\dfrac{g}{f}\right)(2) = \dfrac{g(2)}{f(2)} = \dfrac{-2}{0} =$ not allowed $\implies 2 \notin \mathrm{Dom}(g/f)$
5. $\left(\dfrac{g}{f}\right)(1) = \dfrac{g(1)}{f(1)} = \dfrac{-3}{-15} = \frac{1}{5}$

Function Composition

Definition 5 (Function Composition)

Let $f : A \to B$ and $g : B \to C$. Then the composition of f followed by g, written $g \circ f$ is a function from A into C defined by

$$(g \circ f)(x) = g(f(x))$$

which is read as "g of f of x" or "g after f of x"

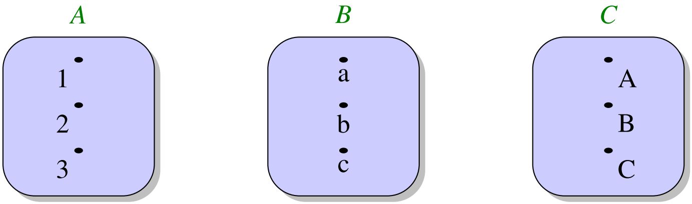
Function Composition

Definition 5 (Function Composition)

Let $f : A \to B$ and $g : B \to C$. Then the composition of f followed by g, written $g \circ f$ is a function from A into C defined by

$$(g \circ f)(x) = g(f(x))$$

which is read as "g of f of x" or "g after f of x"



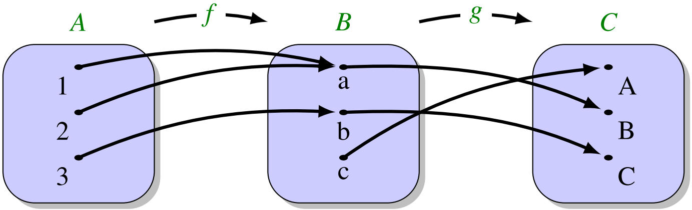
Function Composition

Definition 5 (Function Composition)

Let $f : A \to B$ and $g : B \to C$. Then the composition of f followed by g, written $g \circ f$ is a function from A into C defined by

$$(g \circ f)(x) = g(f(x))$$

which is read as "g of f of x" or "g after f of x"



$f = \{(1, a), (2, a), (3, b)\}$ $\quad$ $g = \{(a, B), (b, C), (c, A)\}$

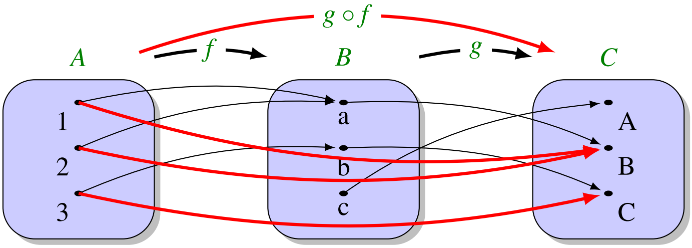
Function Composition

Definition 5 (Function Composition)

Let $f : A \to B$ and $g : B \to C$. Then the composition of f followed by g, written $g \circ f$ is a function from A into C defined by

$$(g \circ f)(x) = g(f(x))$$

which is read as “g of f of x” or “g after f of x”



$f = \{(1,a),(2,a),(3,b)\}$ $g = \{(a,B),(b,C),(c,A)\}$

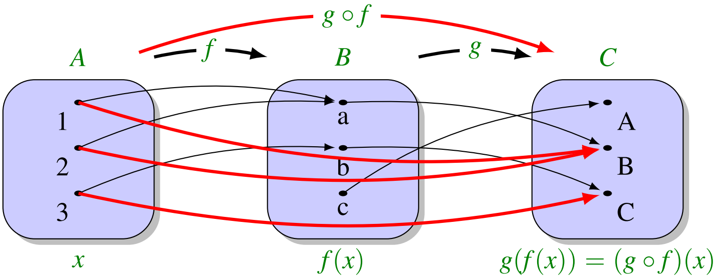
Function Composition

Definition 5 (Function Composition)

Let $f : A \to B$ and $g : B \to C$. Then the composition of f followed by g, written $g \circ f$ is a function from A into C defined by

$$(g \circ f)(x) = g(f(x))$$

which is read as "g of f of x" or "g after f of x"



$f = \{(1, a), (2, a), (3, b)\}$ $g = \{(a, B), (b, C), (c, A)\}$

$g \circ f = \{(1, B), (2, B), (3, C)\}$

Example 6

Example 6 (Function composition using formulae)

Consider functions $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^3$ and $g : \mathbb{R} \to \mathbb{R} : x \mapsto 3x + 1$. Then, construct functions $g \circ f$ and $f \circ g$.

$g \circ f$

$$g \circ f : \mathbb{R} \to \mathbb{R} : x \mapsto g(f(x))$$

and since $g(f(x)) = g(x^3) = 3\left[x^3\right] + 1$ we have

$$g \circ f : \mathbb{R} \to \mathbb{R} : x \mapsto 3x^3 + 1$$

$f \circ g$

$$f \circ g : \mathbb{R} \to \mathbb{R} : x \mapsto f(g(x))$$

and since $f(g(x)) = f(3x + 1) = \left[3x + 1\right]^3$ we have

$$f \circ g : \mathbb{R} \to \mathbb{R} : x \mapsto 27x^3 + 27x^2 + 9x + 1$$

- Note that, in general, $f \circ g \neq g \circ f$.

Example 6

Example 6 (Function composition using formulae)

Consider functions $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^3$ and $g : \mathbb{R} \to \mathbb{R} : x \mapsto 3x + 1$. Then, construct functions $g \circ f$ and $f \circ g$.

$g \circ f$

$$g \circ f : \mathbb{R} \to \mathbb{R} : x \mapsto g(f(x))$$

and since $g(f(x)) = g(x^3) = 3\left[x^3\right] + 1$ we have

$$g \circ f : \mathbb{R} \to \mathbb{R} : x \mapsto 3x^3 + 1$$

$f \circ g$

$$f \circ g : \mathbb{R} \to \mathbb{R} : x \mapsto f(g(x))$$

and since $f(g(x)) = f(3x + 1) = \left[3x + 1\right]^3$ we have

$$f \circ g : \mathbb{R} \to \mathbb{R} : x \mapsto 27x^3 + 27x^2 + 9x + 1$$

- Note that, in general, $f \circ g \neq g \circ f$.

Example 6

Example 6 (Function composition using formulae)

Consider functions $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^3$ and $g : \mathbb{R} \to \mathbb{R} : x \mapsto 3x + 1$. Then, construct functions $g \circ f$ and $f \circ g$.

$g \circ f$

$$g \circ f : \mathbb{R} \to \mathbb{R} : x \mapsto g(f(x))$$

and since $g(f(x)) = g(x^3) = 3\left[x^3\right] + 1$ we have

$$g \circ f : \mathbb{R} \to \mathbb{R} : x \mapsto 3x^3 + 1$$

$f \circ g$

$$f \circ g : \mathbb{R} \to \mathbb{R} : x \mapsto f(g(x))$$

and since $f(g(x)) = f(3x + 1) = \left[3x + 1\right]^3$ we have

$$f \circ g : \mathbb{R} \to \mathbb{R} : x \mapsto 27x^3 + 27x^2 + 9x + 1$$

- Note that, in general, $f \circ g \neq g \circ f$.

Properties of Function Composition

While the previous example shows that we cannot change the order of functions in a function composition we are free to change the grouping ...

Theorem 7 (Function composition is associative)

Given three function, $f : A \to B$, $g : B \to C$, and $h : C \to D$, then

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

- This result means that no matter how the functions in the expression $h \circ g \circ f$ are grouped, the final image of any element of $x \in A$ is $h(g(f(x)))$

Using function composition we can define repeated application of functions[§] ...

Definition 8 ("Powers" of Functions)

Let $f : A \to A$.

- $f^1 = f$; that is, $f^1(a) = f(a)$, for $a \in A$.
- For $n \geq 1$, $f^{n+1} = f \circ f^n$; that is, $f^{n+1}(a) = f\left(f^n(a)\right)$ for $a \in A$.

[§] Take care of notation here: $f^2(x) \neq (f(x))^2$, etc.

Properties of Function Composition

While the previous example shows that we cannot change the order of functions in a function composition we are free to change the grouping ...

Theorem 7 (Function composition is associative)

Given three function, $f : A \to B$, $g : B \to C$, and $h : C \to D$, then

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

- This result means that no matter how the functions in the expression $h \circ g \circ f$ are grouped, the final image of any element of $x \in A$ is $h(g(f(x)))$

Using function composition we can define repeated application of functions[§] ...

Definition 8 ("Powers" of Functions)

Let $f : A \to A$.

- $f^1 = f$; that is, $f^1(a) = f(a)$, for $a \in A$.
- For $n \geq 1$, $f^{n+1} = f \circ f^n$; that is, $f^{n+1}(a) = f\left(f^n(a)\right)$ for $a \in A$.

[§]Take care of notation here: $f^2(x) \neq (f(x))^2$, etc.

Outline

Inverse of a Function

Definition 9 (Inverse of a Function)

Let $f : A \to B$. If there exists a function $g : B \to A$ such that

$$(g \circ f)(x) = x \quad \forall x \in A \qquad \text{and} \qquad (f \circ g)(x) = x \quad \forall x \in B$$

then g is called the inverse of f and is denoted by f^{-1}, read "f inverse".

- Notice that in the definition we refer to "the inverse" as opposed to "an inverse" because, if the inverse exists it is unique.
- The inverse effectively "undoes" the effect of f.

$$\boxed{\text{If } f(a) = b \text{ then } f^{-1}(b) = a}$$

- The inverse of f exists if and only if f is bijective, i.e., f is one-to-one and onto.
- Existence of a function inverse is fundamental to cryptography, lossless compression, relational databases, communication protocols, etc.
- Existence implies nothing about the relative ease of obtaining f^{-1}, or if found the effort to compute $f^{-1}(x)$.

Inverse of a Function

Definition 9 (Inverse of a Function)

Let $f : A \to B$. If there exists a function $g : B \to A$ such that

$$(g \circ f)(x) = x \quad \forall x \in A \qquad \text{and} \qquad (f \circ g)(x) = x \quad \forall x \in B$$

then g is called the inverse of f and is denoted by f^{-1}, read "f inverse".

- Notice that in the definition we refer to "the inverse" as opposed to "an inverse" because, if the inverse exists it is unique.
- The inverse effectively "undoes" the effect of f.

$$\boxed{\text{If } f(a) = b \text{ then } f^{-1}(b) = a}$$

- The inverse of f exists if and only if f is bijective, i.e., f is one-to-one and onto.
- Existence of a function inverse is fundamental to cryptography, lossless compression, relational databases, communication protocols, etc.
- Existence implies nothing about the relative ease of obtaining f^{-1}, or if found the effort to compute $f^{-1}(x)$.

Inverse of a Function

Definition 9 (Inverse of a Function)

Let $f : A \to B$. If there exists a function $g : B \to A$ such that

$$(g \circ f)(x) = x \quad \forall x \in A \qquad \text{and} \qquad (f \circ g)(x) = x \quad \forall x \in B$$

then g is called the inverse of f and is denoted by f^{-1}, read "f inverse".

- Notice that in the definition we refer to "the inverse" as opposed to "an inverse" because, if the inverse exists it is unique.
- The inverse effectively "undoes" the effect of f.

$$\boxed{\text{If } f(a) = b \text{ then } f^{-1}(b) = a}$$

- The inverse of f exists if and only if f is bijective, i.e., f is one-to-one and onto.
- Existence of a function inverse is fundamental to cryptography, lossless compression, relational databases, communication protocols, etc.
- Existence implies nothing about the relative ease of obtaining f^{-1}, or if found the effort to compute $f^{-1}(x)$.

Inverse of a Function

Definition 9 (Inverse of a Function)

Let $f : A \to B$. If there exists a function $g : B \to A$ such that

$$(g \circ f)(x) = x \quad \forall x \in A \qquad \text{and} \qquad (f \circ g)(x) = x \quad \forall x \in B$$

then g is called the inverse of f and is denoted by f^{-1}, read "f inverse".

- Notice that in the definition we refer to "the inverse" as opposed to "an inverse" because, if the inverse exists it is unique.
- The inverse effectively "undoes" the effect of f.

$$\boxed{\text{If } f(a) = b \text{ then } f^{-1}(b) = a}$$

- The inverse of f exists if and only if f is bijective, i.e., f is one-to-one and onto.
- Existence of a function inverse is fundamental to cryptography, lossless compression, relational databases, communication protocols, etc.
- Existence implies nothing about the relative ease of obtaining f^{-1}, or if found the effort to compute $f^{-1}(x)$.

Inverse of a Function

Definition 9 (Inverse of a Function)

Let $f : A \to B$. If there exists a function $g : B \to A$ such that

$$(g \circ f)(x) = x \quad \forall x \in A \qquad \text{and} \qquad (f \circ g)(x) = x \quad \forall x \in B$$

then g is called the inverse of f and is denoted by f^{-1}, read "f inverse".

- Notice that in the definition we refer to "the inverse" as opposed to "an inverse" because, if the inverse exists it is unique.
- The inverse effectively "undoes" the effect of f.

  If $f(a) = b$ then $f^{-1}(b) = a$

- The inverse of f exists if and only if f is bijective, i.e., f is one-to-one and onto.
- Existence of a function inverse is fundamental to cryptography, lossless compression, relational databases, communication protocols, etc.
- Existence implies nothing about the relative ease of obtaining f^{-1}, or if found the effort to compute $f^{-1}(x)$.

Inverse of a Function

Definition 9 (Inverse of a Function)

Let $f : A \to B$. If there exists a function $g : B \to A$ such that

$$(g \circ f)(x) = x \quad \forall x \in A \qquad \text{and} \qquad (f \circ g)(x) = x \quad \forall x \in B$$

then g is called the inverse of f and is denoted by f^{-1}, read "f inverse".

- Notice that in the definition we refer to "the inverse" as opposed to "an inverse" because, if the inverse exists it is unique.
- The inverse effectively "undoes" the effect of f.

$$\boxed{\text{If } f(a) = b \text{ then } f^{-1}(b) = a}$$

- The inverse of f exists if and only if f is bijective, i.e., f is one-to-one and onto.
- Existence of a function inverse is fundamental to cryptography, lossless compression, relational databases, communication protocols, etc.
- Existence implies nothing about the relative ease of obtaining f^{-1}, or if found the effort to compute $f^{-1}(x)$.

Example 10

Example 10

On the set $A = \{0, 1, 2, 3, 4\}$ the functions

$$f : A \to A : x \mapsto -\frac{5}{6}x^4 + \frac{20}{3}x^3 - \frac{50}{3}x^2 + \frac{83}{6}x$$

and

$$g : A \to A : x \mapsto 2x \bmod 5$$

are inverse functions.

Example 10

Example 10

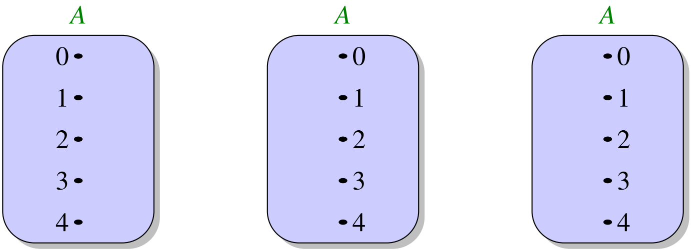
On the set $A = \{0, 1, 2, 3, 4\}$ the functions

$$f : A \to A : x \mapsto -\frac{5}{6}x^4 + \frac{20}{3}x^3 - \frac{50}{3}x^2 + \frac{83}{6}x$$

and

$$g : A \to A : x \mapsto 2x \bmod 5$$

are inverse functions.



Example 10

Example 10

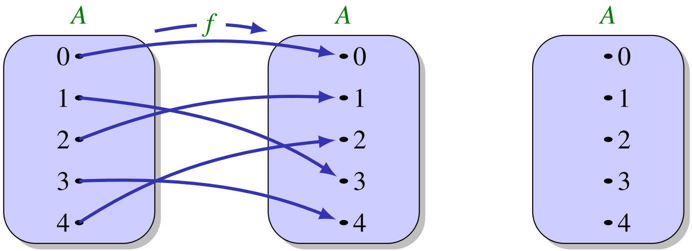
On the set $A = \{0, 1, 2, 3, 4\}$ the functions

$$f : A \to A : x \mapsto -\frac{5}{6}x^4 + \frac{20}{3}x^3 - \frac{50}{3}x^2 + \frac{83}{6}x$$

and

$$g : A \to A : x \mapsto 2x \bmod 5$$

are inverse functions.



Example 10

Example 10

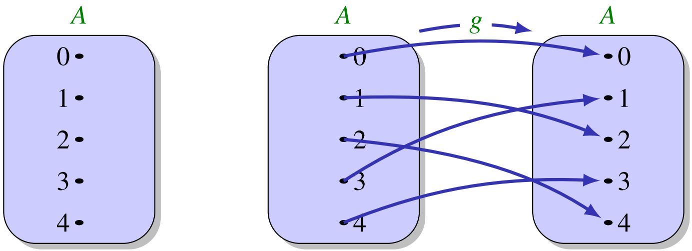
On the set $A = \{0, 1, 2, 3, 4\}$ the functions

$$f : A \to A : x \mapsto -\frac{5}{6}x^4 + \frac{20}{3}x^3 - \frac{50}{3}x^2 + \frac{83}{6}x$$

and

$$g : A \to A : x \mapsto 2x \bmod 5$$

are inverse functions.



Example 10

Example 10

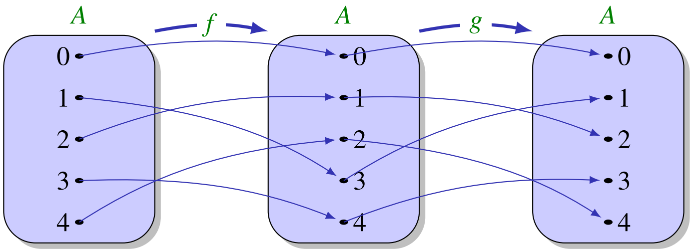
On the set $A = \{0, 1, 2, 3, 4\}$ the functions

$$f : A \to A : x \mapsto -\frac{5}{6}x^4 + \frac{20}{3}x^3 - \frac{50}{3}x^2 + \frac{83}{6}x$$

and

$$g : A \to A : x \mapsto 2x \bmod 5$$

are inverse functions.



Example 10

Example 10

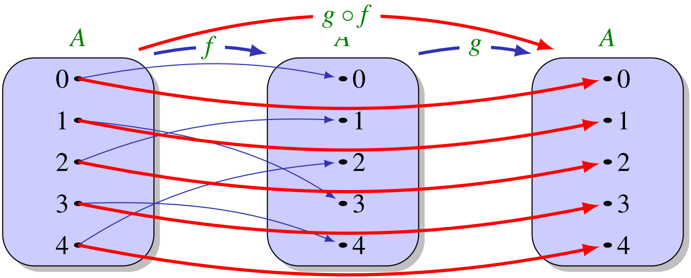
On the set $A = \{0, 1, 2, 3, 4\}$ the functions

$$f : A \to A : x \mapsto -\frac{5}{6}x^4 + \frac{20}{3}x^3 - \frac{50}{3}x^2 + \frac{83}{6}x$$

and

$$g : A \to A : x \mapsto 2x \bmod 5$$

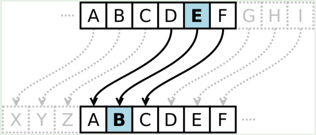
are inverse functions.



Example — Caesar Cipher I

Example 11 (Caesar Cipher)

The Caesar cipher, also known as a shift cipher, is one of the simplest forms of encryption. It is a substitution cipher where each letter in the original message (called the plaintext) is replaced with corresponding letter at a fixed shift¶ in the alphabet with wrap around.



Decrypting with shift of 3.

If n is the required shift, and we have functions to map letters to/from integers such that 'A' $\leftrightarrow 0$, 'B' $\leftrightarrow 1, \ldots,$ 'Z' $\leftrightarrow 25$ then we have inverse function pair

$$E_n(x) = (x + n) \bmod 26$$

and

$$D_n(x) = (x - n) \bmod 26$$

In other words, $(D_n \circ E_n)(x) = x$

¶Apparently Caesar used to prefer an offset of 3 letters, and would shave slaves' head, tattoo encrypted message, wait till hair regrows and then send "message".

Example — Caesar Cipher II

Application

Caesar's used[‖] a shift of 3 so had encrypt/decrypt inverse pair E_3 and D_3,

$$
E_3 \downarrow \quad
\begin{array}{cccccccccccccccccccccccccc}
A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\
\updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\
D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z & A & B & C
\end{array}
\quad \uparrow D_3
$$

The following message was encrypted using E_3

$$V\,H\,Q\,G \quad P\,R\,U\,H \quad I\,R\,R\,G$$

Decrypt the message

$$\_\,\_\,\_\,\_ \quad \_\,\_\,\_\,\_ \quad \_\,\_\,\_\,\_$$

[‖] Security-wise, this is worse than useless, and has not been used since the 16th century, but a shift of 13 was (is?) popular in usenet newsgroups when posting offensive content. Google "ROT13"

Example — Caesar Cipher III

Implementation

If n is the required shift, then using the ord and chr functions in Python** we have inverse function pair

$$E_n(c) = \underbrace{\mathrm{chr}\left(\underbrace{\left(\underbrace{\underbrace{\left(\underbrace{\mathrm{ord}(c) - \mathrm{ord}('A')}_{\text{get integer in range } 0 \ldots 25} + n \right)}_{\text{apply shift}} \bmod 26}_{\text{apply wrap around}} \right) + \mathrm{ord}('A')}_{\text{Add back ASCII offset}} \right)}_{\text{convert back to uppercase character}}$$

and decrypt function

$$D_n(c) = \mathrm{chr}\left(\left(\left(\mathrm{ord}(c) - \mathrm{ord}('A') + (26 - n) \right) \bmod 26 \right) + \mathrm{ord}('A') \right) = E_{26-n}(x)$$

**These functions map to/from ASCII values, so we have 'A' $\leftrightarrow$ 65, 'B' $\leftrightarrow$ 66, . . . , 'Z' $\leftrightarrow$ 90

Example — Caesar Cipher IV

caesar.py

```python
def shift (n, x):
    return (x+n) % 26

def encrypt(n,message):
    result = ""
    for c in message:
        if 'A'<=c<='Z':
            result += chr(shift(n, ord(c)-ord('A')) + ord('A'))
        else:
            result += c
    return result
```

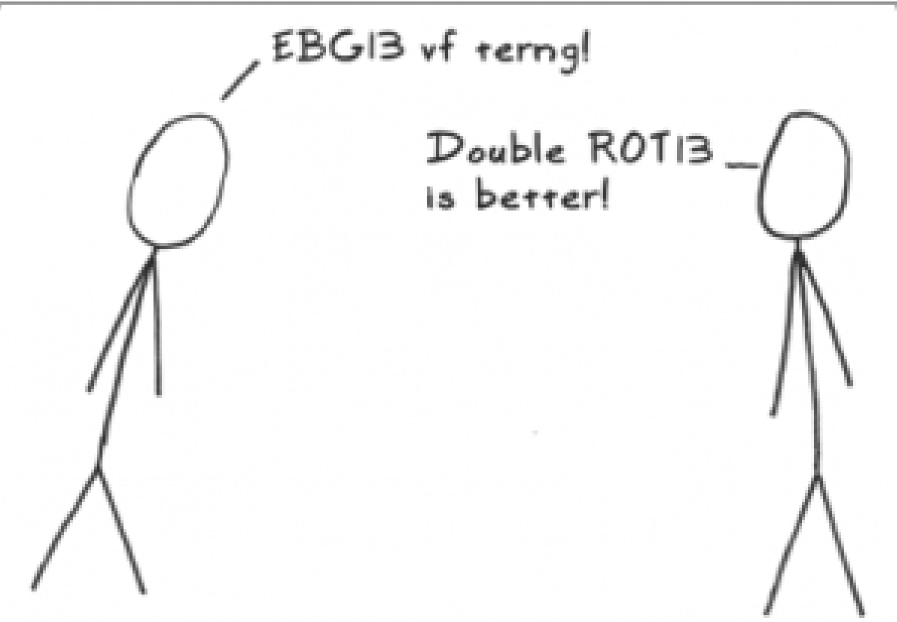
caesar.py

```python
plaintext = "ATTACK AT DAWN"
cypertext = encrypt(3, plaintext)
test = decrypt(3, cypertext)

print ("Plaintext = ", plaintext)
print ("Cypertext = ", cypertext)
print ("test      = ", test)
```

```
Plaintext =  ATTACK AT DAWN
Cypertext =  DWWDFN DW GDZQ
test      =  ATTACK AT DAWN
```

ROT13



Review Exercises 1 (Function Inverse)

Question 1:
Let $A = \{1, 2, 3\}$. Define $f : A \to A$ by $f(1) = 2, f(2) = 1$, and $f(3) = 3$. Find f^2 , f^3 , f^4 and f^{-1}.

Question 2:
Let f, g, and h all be functions from $\mathbb{Z}$ into $\mathbb{Z}$ defined by $f(n) = n + 5$, $g(n) = n - 2$, and $h(n) = n^2$.
Define:

(a) $f \circ g$

(b) f^3

(c) $f \circ h$

Question 3:
Define s, u, and d, all functions on the set of integers, $\mathbb{Z}$, by $s(n) = n^2$, $u(n) = n + 1$, and $d(n) = n - 1$. Determine:

(a) $u \circ s \circ d$

(b) $s \circ u \circ d$

(c) $d \circ s \circ u$

Question 4:
Define the following functions on the integers by $f(k) = k + 1$, $g(k) = 2k$, and $h(k) = \lceil k/2 \rceil$

(a) Which of these functions are one-to-one?

(b) Which of these functions are onto?

(c) Express in simplest terms the compositions $f \circ g$, $g \circ f$, $g \circ h$, $h \circ g$, and h^2 ,