Discrete Mathematics, Section 001, Fall 2016

Lecture 16: Composition of functions, Operations, Symmetries

Zsolt Pajor-Gyulai
zsolt@cims.nyu.edu

Courant Institute of Mathematical Sciences

November 7, 2016

Outline

1. Composition
2. Operations
3. Symmetries

The natural operation to combining functions

Definition

Let A, B, and C be sets and let $f : A \to B$ and $g : B \to C$. Then $g \circ f : A \to C$ is defined by

$$(g \circ f)(a) = g[f(a)], \qquad a \in A.$$

The function $g \circ f$ is called **the composition** of g and f.

For example, let

$$A = \{1, 2, 3, 4, 5\} \qquad B = \{6, 7, 8, 9\} \qquad C = \{10, 11, 12, 13, 14\}.$$

Let

$$f = \{(1, 6), (2, 6), (3, 9), (4, 7), (5, 7)\}$$
$$g = \{(6, 10), (7, 11), (8, 12), (9, 13)\}.$$

Then

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

Further example

Let $f : \mathbb{Z} \to \mathbb{Z}$ and $g : \mathbb{Z} \to \mathbb{Z}$ defined by

$$f(x) = x^2 + 1, \qquad g(x) = 2x - 3$$

Then

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

Remarks:

- Note the order in $(g \circ f)(a)$. f is closer and hits a first.
- $\mathrm{Dom}(g \circ f) = \mathrm{Dom} f$.

$$f : A \to B, \qquad g : B \to C \qquad \to \qquad \mathrm{Im} f \subseteq B = \mathrm{Dom} g$$

Q: Is $f \circ g = g \circ f$?

- This only makes sense in the first place if $f : A \to A$ and $g : A \to A$.
- Even then, this is not true in general!

For example, let $A = \{1, 2, 3, 4, 5, 6\}$ and $f : A \to A$, $g : A \to A$ defined by

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

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

Then

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

Thus

$$g \circ f \neq f \circ g$$

Another example, $f, g : \mathbb{Z} \to \mathbb{Z}$

$$f(x) = x^2 + 1, \qquad g(x) = 2x - 3$$

Then

$$(g \circ f)(x) = g[f(x)] = g[x^2 + 1] = 2(x^2 + 1) - 3 = 2x^2 - 1$$

$$(f \circ g)(x) = f[g(x)] = f[2x - 3] = (2x - 3)^2 + 1 = 4x^2 - 12x + 10$$

Once again

$$g \circ f \neq f \circ g$$

Composition is not commutative!

Do Problem 1 on the WS!

What about associativity?

Proposition

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

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

To prove this we need to prove the equality of functions.

Proving two functions are equal

Let f and g be functions. To prove $f = g$, do the following:

- Prove that $\mathrm{Dom} f = \mathrm{Dom} g$.
- Prove that for all x in the common domain, $f(x) = g(x)$.

Proposition

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

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

Proof.

We first check that the domains are the same.

$$\mathrm{Dom}[h \circ (g \circ f)] = \mathrm{Dom}(g \circ f) = \mathrm{Dom} f = A$$

$$\mathrm{Dom}[(h \circ g) \circ f] = \mathrm{Dom} f = A$$

Then we check that they have the same values. For $a \in A$,

$$[h \circ (g \circ f)](a) = h[(g \circ f)(a)] = h[g(f(a))]$$

$$[(h \circ g) \circ f](a) = (h \circ g)[f(a)] = h[g(f(a))]$$

This finishes the proof of the proposition. $\square$

Identity function

Definition

Let A be a set. The **identity function** on A is the function $\mathrm{id}_A : A \to A$, defined by $\mathrm{id}_A(a) = a$. In other words,

$$\mathrm{id}_A = \{(a, a) : a \in A\}.$$

If composition is the analogue of a product, then id_A is the analogue of ‘one‘.

Proposition

Let A and B be sets. Let $f : A \to B$. Then

$$f \circ \mathrm{id}_A = \mathrm{id}_B \circ f = f$$

Identity function

Proposition

Let A and B be sets. Let $f : A \to B$. Then

$$f \circ \mathrm{id}_A = \mathrm{id}_B \circ f = f$$

Proof.

We first show they have the same domain:

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

$$\mathrm{Dom}(\mathrm{id}_B \circ f) = \mathrm{Dom} f = A$$

Second, observe

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

and $(\mathrm{id}_B \circ f)(a) = f(a)$ similarly and the claim is proved. □

Do Problem 2 on the WS!

Outline

General notion of an operation

Abstract algebra is the study of structures and operations.

Definition

Let A be a set. A **binary operation** on A is a function whose domain is $A \times A$.

For example,

- $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $+(a, b) = a + b$.
- $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $f(x, y) = |x - y|$

Commonly used symbol for operations: $*$
Notation: $*(a, b) = a * b$.

When we want to emphasize what the set A is, we use the notation $(A, *)$. The two above examples then are

$$(\mathbb{R}, +), \qquad (\mathbb{Z}, f)$$

Other examples

- $+$ is an operation on $\mathbb{N}$ and $a + b \in \mathbb{N}$ whenever $a, b \in \mathbb{N}$. (**closure property**)
- $-$ is an operation on $\mathbb{N}$ but $a - b$ might not be a natural for every $a, b \in \mathbb{N}$.
- $\cdot$ is an operation on $\mathbb{N}$ and the closure property holds.
- $/$ is not an operation on $\mathbb{N}$ as e.g. $(2, 0)$ is not in its domain.
- $/$ is, however, a relation on the positive integers.
- $\circ$ is an operation on the set of functions from A^A (set of functions from A to A).

This week, we are going to learn about another interesting examples: permutations.

Properties of operations

Commutative property

Let $*$ be an operation on a set A. We say that * is **commutative** on A provided

$$\forall a, b \in A, a * b = b * a$$

For example,

- $+$ is commutative on $\mathbb{Z}$
- $\circ$ is not commutative on A^A.
- $-$ is not commutative on $\mathbb{Z}$.

Properties of operations

Closure property

Let $*$ be an operation on a set A. We say that $*$ is closed on A provided

$$\forall a, b \in A, a * b \in A$$

For example,

- $\cdot$ is closed on $\mathbb{N}$
- $-$ is not closed on $\mathbb{N}$
- $-$ is closed on $\mathbb{Z}$.

Properties of operations

Associative property

Let $*$ be an operation on a set A. We say that $*$ is **associative** on A provided

$$\forall a, b, c \in A, (a * b) * c = a * (b * c).$$

For example,

- $+$ and $\cdot$ are associative on $\mathbb{Z}$
- $-$ is not as e.g.

$$(3 - 4) - 7 = -8 \neq 6 = 3 - (4 - 7)$$

Properties of operations

Identity element

Let $*$ be an operation on a set A. An element $e \in A$ is called an **identity** for $*$ provided

$$\forall a \in A, a * e = e * a = a$$

For example,

- 0 is an identity element for $+$ on $\mathbb{Z}$
- 1 is an identity element for $\cdot$ on $\mathbb{Z}$.
- $-$ does not have an identity element on $\mathbb{Z}$ as

$$a - 0 = a, \qquad \text{but} \qquad 0 - a = -a \neq a$$

Properties of operations

Identity element

Let $*$ be an operation on a set A. An element $e \in A$ is called an **identity** for $*$ provided

$$\forall a \in A, a * e = e * a = a$$

Proposition

Let $*$ be an operation defined on a set A. Then $*$ can have at most one identity elements.

FTSC, suppose there are two identities e and e' in A with $e \neq e'$.

- On one hand $e * e' = e$ as e' is an identity.
- On the other hand $e * e' = e'$ as e is an identity.

Therefore $e = e'$ contradicting $e \neq e'$. $\Rightarrow\Leftarrow$

Properties of operations

Inverses

Let $*$ be an operation on a set A and suppose A has an identity e. For an element $a \in A$, we call an element $b \in A$ an **inverse** of a provided $a * b = b * a = e$.

For example,

- In $(\mathbb{Z}, +)$, the inverse of $a \in \mathbb{Z}$ is $(-a)$.
- In $(\mathbb{Q}, \cdot)$, the inverse of $x \in \mathbb{Q}$ is $\frac{1}{x}$ when $x \neq 0$. However $x = 0$ does not have an inverse!
- Consider the following relation on $\{e, a, b, c\}$:

*	e	a	b	c
e	e	a	b	c
a	a	a	e	e
b	b	e	b	e
c	c	e	e	c

Both b and c are inverses of a:

$$a * b = b * a = e, \qquad a * c = c * a = e$$

The inverse might not be unique.

Do Problem 3 on the WS!

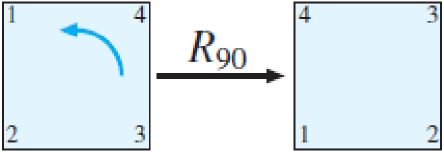
Outline

Symmetries of the square

Intuitively

A **symmetry** of a figure is a motion that, when applied to an object, results in a figure that looks exactly the same as the original

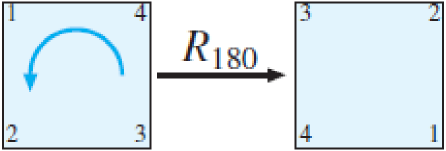
- Rotating a square counterclockwise about its center through an angle of 90° is a symmetry.



- However, rotating by 30°, denoted by R_{30} is not a symmetry.

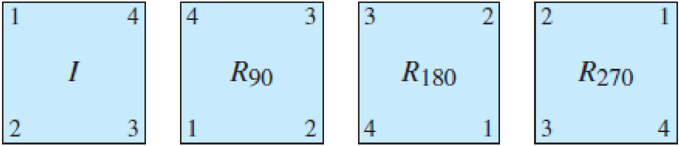
Symmetries of the square

- In the same vein, R_{180}, R_{270}, and R_{360} are also symmetries. E.g.:



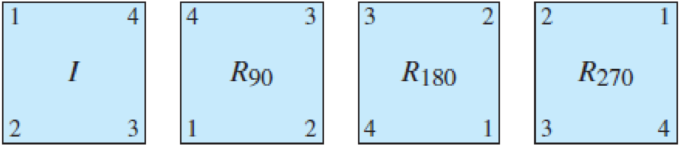
- However, we would rather like to say that R_{360} does not do anything, and we are going to call it I for identity.

With this, we have the following symmetries:



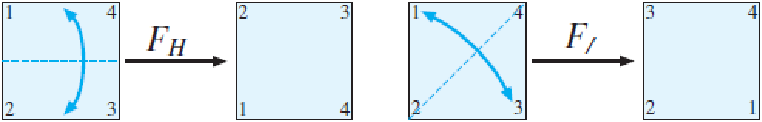
Symmetries of the square

With this, we have the following symmetries:



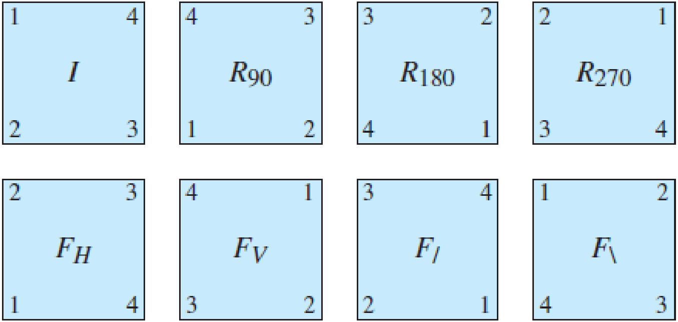
However, we have more symmetries: reflections.

- For example, reflection through the horizontal axis and the *SW* – *NE* diagonal:



- Of course we have to more axis to reflect about: $-$, $\backslash$

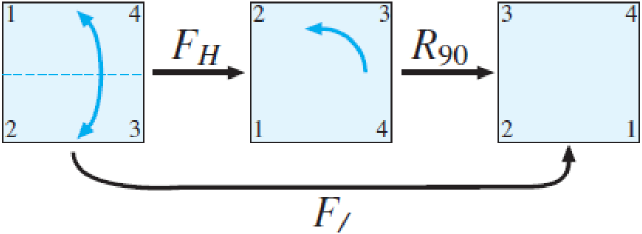
Symmetries of the square



- **Have we repeated ourselves?** No, notice that no two corner label arrangements are the same.
- **Did we find all symmetries?** Yes, we exhausted all possible $2 \cdot 4 = 8$ label arrangements. (Label 1 can go to four places, after which for label 2, we have two choices, after which $3, 4$ are fixed.)

Combining symmetries

Applying symmetries consecutively, the result will also be a symmetry. For example,



Since the result is a symmetry it must be one of the 8 ones that we have listed!

$$R_{90} \circ F_H = F_I$$

where the left hand side means applying F_H first and then R_{90}.

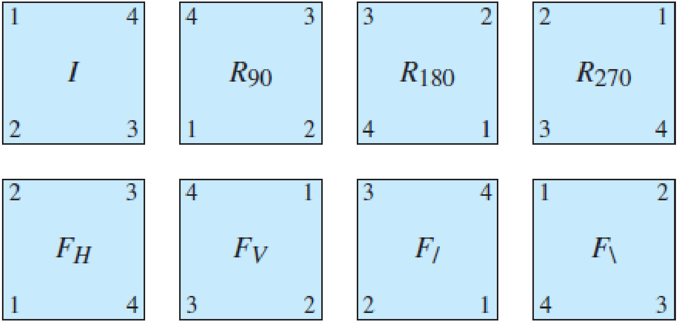
'Multiplication table for the symmetries of squares'

If we figure out all the combinations:

$\circ$	I	R_{90}	R_{180}	R_{270}	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

- Note that, $R_{90} \circ F_H = F_{/} \neq F_{\backslash} = F_H \circ R_{90}$, and therefore $\circ$ is not commutative.
- I is the identity element for $\circ$.
- Every element has an inverse.

Symmetries as permutations



- Note that if I tell you where the labels $1, 2, 3, 4$ go, you can identify the symmetry!
- For example, R_{90} can be represented as a function

$$R_{90} : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$$

$$R_{90}(1) = 2, \qquad R_{90}(2) = 3, \qquad R_{90}(3) = 4, \qquad R_{90}(4) = 1$$

Symmetries as permutations

Symmetry name	1	2	3	4
	go to positions			
I	1	2	3	4
R_{90}	2	3	4	1
R_{180}	3	4	1	2
R_{270}	4	1	2	3
F_H	2	1	4	3
F_V	4	3	2	1
$F_/$	3	2	1	4
$F_\backslash$	1	4	3	2

Convenient notation:

$$R_{90} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} \qquad F_H = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}$$