CSCI/MATH 2113 Discrete Structures

Chapter 5 Relations and Functions

Alyssa Motas

March 2, 2021

Contents

1 (5.1) Cartesian Products and Relations

1.1 Cartesian Product

1.1.1 Definition

For sets A, B the *Cartesian product*, or *cross product*, of A and B is denoted by $A \times B$ and equals $\{(a,b) \mid a \in A, b \in B\}$.

1.1.2 Example

Suppose that $A = \{2,3,4\}$ and $B = \{4,5\}$ then we have

$$A \times B = \{(2,4),(2,5),(3,4),(3,5),(4,4),(4,5)\}.$$

Note that

$$A \times B \neq B \times A.$$

Another example of a Cartesian product is the real plane $\mathbb{R} \times \mathbb{R}$.

1.1.3 Notation

$$A^n = \underbrace{A \times A \times A \times \cdots \times A}_{n \text{ times}}.$$

1.2 Relations

1.2.1 Definition

For sets A, B, any subset of $A \times B$ is called a (*binary*) *relation* from A to B. Any subset of $A \times A$ is called a (*binary*) *relation* on A.

1.2.2 Notation

If R is a relation on A and $(a, a') \in R$, then we write aRa'.

1.2.3 Examples

Suppose that $A = \{2,3,4\}$ and $B = \{4,5\}$. Then,

- $\{(2,5),(2,4)\}$
- $A \times B$
- $\varnothing$

are relations from A to B.

1.2.4 Counting

For finite sets A, B with $|A| = m$ and $|B| = n$, there are 2^{mn} relations from A to B, including the empty relation as well as the relation $A \times B$ itself.

There are also $2^{nm} (= 2^{mn})$ relations from B to A, one of which is also $\varnothing$ and another of which is $B \times A$. The reason we get the same number of relations from B to A as we have from A to B is that any relation R_1 from B to A can be obtained from a unique relation R_2 from A to B by simply reversing the components of each ordered pair in R_2 (and vice versa).

1.2.5 Standard Relations

Standard relations can be expressed in this way:

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b = a + n \text{ for } n \in \mathbb{N}\}.$$

This is the relation "is less than or equal to." Indeed

$$(a, b) \in R \text{ if and only if } a \leq b.$$

Suppose that $A = \{1\}$ and let $R \subseteq \mathcal{P}(A)^2$ defined by

$$R = \{(\varnothing, \varnothing), (\varnothing, \{1\}), (\{1\}, \{1\})\}.$$

This is the relation "is a subset of." Indeed,

$$(S, S') \in R \text{ if and only if } S \subseteq S'.$$

1.2.6 Theorem

For sets A, B, and C:

- $A \times \varnothing = \varnothing = \varnothing \times A$
- $A \times (B \cap C) = (A \times B) \cap (A \times C)$
- $A \times (B \cup C) = (A \times B) \cup (A \times C)$
- $(B \cap C) \times A = (B \times A) \cap (C \times A)$
- $(B \cup C) \times A = (B \times A) \cup (C \times A)$

Proof. Let $x \in A \times (B \cap C)$. Then $x = (a, d)$ when $a \in A, d \in B \cap C$. So, $x = (a, d)$ with $a \in A$ and $d \in B$ which implies that $x \in A \times B$. But $x = (a, d)$ with $a \in A$ and $d \in C$, which implies $x \in A \times C$. Hence, we have $x \in (A \times B) \cap (A \times C)$ which implies $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$. The converse inclusion is shown similarly. Hence we have the desired equality. The other statements are proved similarly as well. $\square$

1.2.7 Recursive Relation

An example of a recursively defined relation is on $\mathbb{N} \times \mathbb{N}$:

1. $(0,0) \in R$
2. If $(s,t) \in R$ then $(s+1, t+7) \in R$.

In fact, we have

$$R = \{(m,n) \mid n = 7m\}.$$

2 (5.2) Functions Plain and One-to-One

2.1 Defintion of a function

For nonempty sets A, B, a *function*, or *mapping*, f from A to B, denoted $f : A \to B$, is a relation from A to B in which every lement of A appears exactly once as the first component of an ordered pair in the relation.

We have $f \subseteq A \times B$ and

(1) Existence:

$$\forall a \in A, \exists b \in B, (a,b) \in f.$$

(2) Uniqueness: If $(a,b) \in f$ and $(a,b') \in f$ then

$$b = b'.$$

2.1.1 Image and Preimage

If $(a,b) \in f$, we write $f(a) = b$. We then say that b is the *image* of a under f, and that a is the *preimage* of b under f.

Example. The absolute value is the function $|x| : \mathbb{R} \to \mathbb{R}$. Here, 2 and -2 are two preimages of 2 since

$$|2| = 2 = |-2|.$$

So a given element can have more than one preimage.

2.1.2 Domain and codomain

For the function $f : A \to B$, A is called the *domain* of f and B the *codomain* of f. The subset of B consisting of those elements that appear as second components in the ordered pairs of f is called the *range* of f and is also denoted by $f(A)$ because it is the set of images (of the elements of A) under f.

Note: Range does not imply that it is equal to codomain.

2.1.3 Examples

1. The *greatest integer function*, or *floor function*. This function $f : \mathbb{R} \to \mathbb{R}$, is given by

   $$f(x) = \lfloor x \rfloor = \text{ the greatest integer less than or equal to } x$$

   Example. $\lfloor 7.7 + 8.4 \rfloor = \lfloor 16.1 \rfloor = 16$.

2. The *ceiling function*. This function $g : \mathbb{R} \to \mathbb{Z}$ is defined by

   $$g(x) = \lceil x \rceil = \text{ the least integer greater than or equal to } x.$$

   Example. $\lceil 3.3 + 4.2 \rceil = \lceil 7.5 \rceil = 8$.

3. The function trunc (for truncation). It deletes the fractional part of a real number. Note that trunc(3.78) $= \lfloor 3.78 \rfloor = 3$ while trunc(-3.78) $= \lceil -3.78 \rceil = -3$.

4. The *access* function. In storing a matrix in a one-dimensional array, many computer languages use the *row major* implementation. If $A = (a_{ij})_{m \times n}$ is an $m \times n$ matrix, to determine the location of an entry a_{ij} from A, where $1 \le i \le m, 1 \le j \le n$, we can use the formula for the access function:
   $$f(a_{ij}) = (i-1)n + j.$$

2.1.4 Counting functions

Let A, B be nonempty sets with $|A| = m, |B| = n$. How many functions are there in $f : A \to B$?

Suppose that $A = \{a_1, a_2, a_3, \ldots, a_m\}$ and $B = \{b_1, b_2, b_3, \ldots, b_n\}$, then a typical function can be described by $\{(a_1, x_1), (a_2, x_2), \ldots, (a_m, x_m)\}$. We can select any n elements of B for x_1 then do the same for x_2. We continue this selection until one of the n elements of B is finally selected for x_m. Using the product rule, there are

$$n^m = |B|^{|A|}$$

functions from A to B.

Example. Suppose that $A = \{1, 2, 3\}$ and $B = \{w, x, y, z\}$. There are $4^3 = 64$ functions from A to B.

In general, we do not expect $|A|^{|B|} = |B|^{|A|}$.

2.2 One-to-one Correspondence

2.2.1 Definition

A function $f : A \to B$ is called *one-to-one*, or *injective*, if each element of B appears at most once as the image of an element of A.

If $f : A \to B$ is one-to-one, with A, B finite, we must have $|A| \le |B|$. For arbitrary sets A, B, $f : A \to B$ is one-to-one if and only if for all $a_1, a_2 \in A, f(a_1) = f(a_2) \Rightarrow a_1 = a_2$. Consequently, we also have $a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$.

2.2.2 Examples

1. Suppose that $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = 3x + 7$ for all $x \in \mathbb{R}$. Then for all $x_1, x_2 \in \mathbb{R}$, we find that

   $$f(x_1) = f(x_2) \Rightarrow 3x_1 + 7 = 3x_2 + 7 \Rightarrow 3x_1 = 3x_2 \Rightarrow x_1 = x_2,$$

   so the given function f is one-to-one.

2. Suppose that $g : \mathbb{R} \to \mathbb{R}$ is the function defined by $g(x) = x^4 - x$ for each real number x. Then

   $$g(0) = (0)^4 - 0 = 0 \text{ and } g(1) = (1)^4 - (1) = 1 - 1 = 0.$$

   Consequently, g is not one-to-one since $g(0) = g(1)$ but $0 \neq 1$.

2.2.3 Counting injective functions

Let A, B be nonempty sets with $|A| = m, |B| = n$. How many injective functions are there in $f : A \to B$?

Suppose that $A = \{a_1, \ldots, a_m\}$, $B = \{b_1, \ldots, b_n\}$, and that $m \le n$. The one-to-one function has the form $\{(a_1, x_1), \ldots, (a_m, x_m)\}$, where there are n choices for x_1, $n - 1$ choices for x_2, $n - 2$ choices for x_3, and so on, finishing with $n - (m - 1) = n - m + 1$ choices for x_m. By the rule of product, we have

$$n(n-1)(n-2)\ldots(n-m+1) = \frac{n!}{(n-m)!} = P(n, m) = P(|B|, |A|).$$

2.2.4 Direct Image

If $f : A \to B$ and $A_1 \subseteq A$, then

$$f(A_1) = f[A_1] = \{b \in B \mid b = f(a), \text{ for some } a \in A_1\},$$

and $f(A_1)$ is called the *direct image* of A_1 under f.

Example. Let $g : \mathbb{R} \to \mathbb{R}$ be given by x^2. Then $g(\mathbb{R}) =$ the range of g $= [0, +\infty)$. The *image* of $\mathbb{Z}$ under g is

$$g(\mathbb{Z}) = \{0, 1, 4, 9, 16, \ldots\}$$

and for $A_1 = [-2, 1]$ we get

$$g(A_1) = [0, 4].$$

2.2.5 Set Operations

Let $f : A \to B$, with $A_1, a_2 \subseteq A$. Then

(a) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$;

(b) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$;

(c) $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$ when f is one-to-one.

Proof. Part (b): For each $b \in B, b \in f(A_1 \cap A_2) \Rightarrow b = f(a)$, for some $a \in A_1 \cap A_2 \implies [b = f(a) \text{ for some } a \in A_1]$ and $[b = f(a) \text{ for some } a \in A_2] \Rightarrow b \in f(A_1)$ and $b \in f(A_2) \Rightarrow b \in f(A_1) \cap f(A_2)$, so $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$. □

2.2.6 Restriction

If $f : A \to B$ and $A_1 \subseteq A$, then $f|_{A_1} : A_1 \to B$ is called the *restriction of f to* A_1 if $f|_{A_1}(a) = f(a)$ for all $a \in A_1$.

2.2.7 Extension

Let $A_1 \subseteq A$ and $f : A_1 \to B$. If $g : A \to B$ and $g(a) = f(a)$ for all $a \in A_1$, then we call g an *extension of f to A*.

3 (5.3) Onto Functions Stirling Numbers of the Second Kind

3.1 Surjective Functions

3.1.1 Definition

$f : A \to B$ is *onto* or *surjective* if $\forall b \in B, \exists a \in A$ such that $f(a) = b$.

Remark. A function is onto if its range is equal to the codomain.

If A, B are finite sets, then for an onto function $f : A \to B$ to possibly exist we must have $|A| \leq |B|$.

3.1.2 Examples

- For the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3$ we have: if $x \in \mathbb{R}$, then $f(\sqrt[3]{x}) = (\sqrt[3]{x})^3 = x$. This means that f is onto.
- For the function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^2$ we have: no such $y \in \mathbb{R}$ that satisfies $y^2 = -1$. For instance,

  $$g(x) = x^2 = -9 \Rightarrow r = 3i, -3i \in \mathbb{C}.$$

  Therefore, g is not onto.

3.1.3 Counting

Suppose that $A = \{x, y, z\}$ and $B = \{1, 2\}$. How many $f : A \to B$ are onto?

Proof. The function $f : A \to B$ is not onto if and only if $f(a) = 1$ for all $a \in A$ or $f(a) = 2$ for all $a \in A$. Hence, the number we seek is

$$|B|^{|A|} - 2 = 2^3 - 2 = 6.$$

$\square$

In general, if A and B are sets with $|A| = m$ and $|B| = n$, then this quantity is

$$\sum_{k=0}^{n}(-1)^k \binom{n}{n-k}(n-k)^m$$

onto functions from A to B.

3.2 Stirling Numbers

3.2.1 A combinatorial interpretation

In how many ways can you distribute 4 objects into 3 labelled cotainers with no container empty? We just need to count the number of surjections from A to B. By the previuos formula, this is

$$\sum_{k=0}^{3}(-1)^k \binom{3}{3-k}(3-k)^4 = 36.$$

What if we had the same situation but with containers that aren't labelled? The number of such distributions is

$$S(m,n) = \frac{1}{n!}\sum_{k=0}^{n}(-1)^k \binom{n}{n-k}(n-k)^m$$

where the factor of $\frac{1}{n!}$ corrects for the fact that certain distributions are equivalent.
So $S(m,n)$ is the number of ways to distribute m objects into n identical containers with no container left empty.

3.2.2 Definition

$S(m,n)$ is a *Stirling number* of the 2nd kind.

4 (5.4) Special Functions

4.1 Binary operations

4.1.1 Definition

For any nonempty sets A, B, any function $f : A \times A \to B$ is called *binary operation* on A. If $B \subseteq A$, then the binrary operation is said to be *closed* (on A). (When $B \subseteq A$ we may also say that A is *closed under f*.)

Remark. Similarly, $f : A^n \to B$ is an *n-ary* operation on A. When $n = 1$, the operation is *unary* or *monary*.

4.1.2 Examples of Binary Operations

- For $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $f(a, b) = a - b$, it is a closed binary operation on $\mathbb{Z}$.
- For $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{R}$ defined by $g(a, b) = a^b$, it is a non-closed binary operation.
- For $h : \mathbb{Z} \times \mathbb{Z} \to \mathbb{R}$ defined by $h(a, b) = a + b$, it is a binary operation.
- For $j : \mathcal{P}(A) \times \mathcal{P}(A) \to \mathcal{P}(A)$ defined by $j(S, T) = S \cup T$, it is a closed binary operation.
- For $k : \mathcal{P}(A) \to \mathcal{P}(A)$ defined by $k(S) = S^c$, it is a closed unary operation.

4.1.3 Commutativity and Associativity

Let $f : A \times A \to B$; that is, f is a binary operation on A.

(a) f is said to be *commutative* if $f(a, b) = f(b, a)$ for all $(a, b) \in A \times A$.

(b) When $B \subseteq A$ (that is, when f is closed), f is said tot be *associative* if for all $a, b, c \in A$, $f(f(a, b), c) = f(a, f(b, c))$.

4.1.4 Examples of Commutativity and Associativity

Binary operations that are both commutative and associative:

- $+$ on $\mathbb{Z}$: $n + m = m + n$ and $n + (m + r) = (n + m) + r$
- $\times$ on $\mathbb{Z}$
- $\cup$ on $\mathcal{P}(A)$

Binary operations that are associative but not commutative:

- $\times$ on $Mat_{n\times n}(\mathbb{R})$ which is the multiplication of $n \times n$ real matrices.

Binary operations that are both not commutative and associative:

- $-$ on $\mathbb{Z}$:

$$2 - 3 = -1 \neq 1 = 3 - 2$$
$$((3 - 3) - 2) = -2 \neq 2 = 3 - (3 - 2)$$

4.1.5 Symmetry

Suppose that $f : A \times A \to A$ is a binary operation where $A = \{a_1, \dots, a_n\}$. We can represent f using a *table*.

f	a_1	a_2	$\dots$	a_n
a_1	$f(a_1, a_1)$	$f(a_1, a_2)$		
a_2	$f(a_2, a_1)$			
$\vdots$				
a_n		$f(a_n, a_2)$		$f(a_n, a_n)$

If the operation is commutative, then the table is *symmetric.*
Now let $f : \{a, b, c\} \times \{a, b, c\} \to \{a, b, c\}$ be defined by the table:

f	a	b	c
a	b	a	a
b	a	c	a
c	a	a	c

Here we have

$$f(a, f(b, c)) = f(a, a) = b \neq a = f(a, c) = f(f(a, b), c)$$

so the operation is *not associative* but it is commutative since the table is symmetric.

4.2 Identity Element

4.2.1 Definition

Let $f : A \times A \to B$ be a binary operation on A. An element $x \in A$ is called an *identity* (or *identity element*) for f if $f(a, x) = f(x, a) = a$, for all $a \in A$.

4.2.2 Examples

- 0 for $+$ on $\mathbb{Z}$ since
$$a + 0 = 0 + a = a$$
for all $a \in \mathbb{Z}$.
- I_n (identity matrix) of x on $Mat_{n \times n}(\mathbb{R})$.
- $\varnothing$ for $\cup$ on $\mathcal{P}(A)$.
- A for $\cap$ on $\mathcal{P}(A)$.

4.2.3 Theorem

Let $f : A \times A \to B$ be a binary operation. If f has an identity, then that identity is unique.

Proof. If f has more than one identity, let $x_1, x_2 \in A$ with

$$\begin{aligned} f(a, x_1) &= a = f(x_1, a), && \text{for all } a \in A, \\ f(a, x_2) &= a = f(x_2, a), && \text{for all } a \in A. \end{aligned}$$

Consider x_1 as an element of A and x_2 as an identity. Then $f(x_1, x_2) = x_1$. Now reverse the roles of x_1 and x_2, that is, consider x_2 as an element of A and x_1 as an identity. We find that $f(x_1, x_2) = x_2$. Consequently, $x_1 = x_2$, and f has at most one identity. $\square$

4.3 Projections

For sets A and B, if $D \subseteq A \times B$, then $\pi_A : D \to A$, defined by $\pi_A(a, b) = a$, is called the *projection* on the first coordinate. The function $\pi_B : D \to B$, defined by $\pi_B(a, b) = b$, is called the *projection* on the second coordinate.

4.4 Counting Binary Operations

- For the set $A = \{a, b, c, d\}$, how many closed binary operations are there on A?

  A binary operation is a function $A \times A \to A$. Hence this number is

  $$|A|^{|A| \times |A|} = 4^{16}.$$

  In other words, we need to fill the table below.

	a	b	c	d
a				
b				
c				
d				

  There are 4 choices for each cell.

- How many of these operations are commutative?

  Commutative operations correspond to symmetric tables.

	a	b	c	d
a				
b	x			
c	x	x		
d	x	x	x	

Since only 10 cells need to be filled, there are

$$4^{10}$$

binary operations.

- How many of these operations have a as an identity?

	a	b	c	d
a	a	b	c	d
b	b			
c	c	x		
d	d	x	x	

Since a is the identity, we have $f(d, a) = d$ for every $d \in A$. In total, there are 4^6 such operations since there are 6 cells to fill.

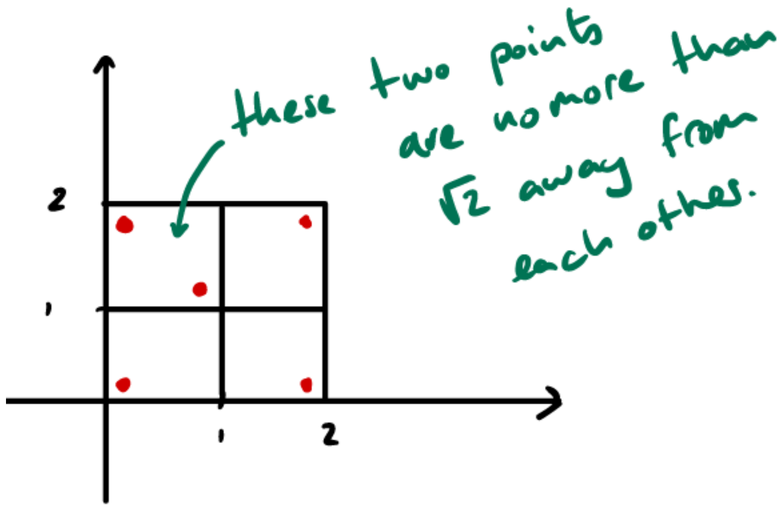
5 (5.5) The Pigeonhole Principle

5.1 Definition

If m pigeons occupy n pigeonholes and $m > n$ then at least one pigeonhole has two or more pigeons in it.

5.2 Example

If there are 5 points in a 2×2 square in the real plane, then two of these points are no more than $\sqrt{2}$ away from each other.



6 (5.6) Function Composition and Inverse Functions

6.1 Bijective functions

If $f : A \to B$, then f is said to be *bijective*, or to be a *one-to-one corespondence*, if f is both one-to-one and onto.

6.2 Identity function

The function $1_A : A \to A$, defined by $1_A(a) = a$ for all $a \in A$, is called the *identity function*.

6.3 Equality of functions

If $f, g : A \to B$, we say that f and g are *equal* and write $f = g$, if $f(a) = g(a)$ for all $a \in A$.
A common pitfall in dealing with the equality of functions occurs when f and g are functions with a common domain A and $f(a) = g(a)$ for all $a \in A$. It may *not* be the case that $f = g$. The pitfall results from not paying attention to the codomains of the functions.

6.3.1 Example

Let $f : \mathbb{Z} \to \mathbb{Z}, g : \mathbb{Z} \to \mathbb{Q}$ where $f(x) = x = g(x)$, for all $x \in \mathbb{Z}$. Then, f, g share the common domain $\mathbb{Z}$, have the same range $\mathbb{Z}$, and act the same on every element of $\mathbb{Z}$. Yet $f \neq g$ because f is injective and g is injective but surjective; so the codomains do not make a difference.

6.4 Composite functions

If $f : A \to B$ and $g : B \to C$, we define the *composite function*, which is denoted $g \circ f : A \to C$, by $(g \circ f)(a) = g(f(a))$, for each $a \in A$. f and g are composable. However, if $C \neq A$ then $f \circ g$ is not defined.

The definition and examples for composite functions required that the codomain of f = domain of g. If range of $f \subseteq g$, this will actually be enough to yield the composite function $g \circ f : A \to C$. Also, for any $f : A \to B$, we observe that $f \circ 1_A = f = 1_B \circ f$.

6.4.1 Theorem

Let $f : A \to B$ and $g : B \to C$.

(a) If f and g are one-to-one, then $g \circ f$ is one-to-one.

(b) If f and g are onto, then $g \circ f$ is onto.

Proof. Let us prove the following theorem above.

(a) Let $a_1, a_2 \in A$ with $(g \circ f)(a_1) = (g \circ f)(a_2)$. Then

$$(g \circ f)(a_1) = (g \circ f)(a_2) \Rightarrow g(f(a_1)) = g(f(a_2)) \Rightarrow f(a_1) = f(a_2)$$

since g is one-to-one. Also, $a_1 = a_2$ because f is one-to-one. Consequently, $g \circ f$ is one-to-one.

(b) Let $z \in C$. Since g is onto, there exists $y \in B$ with $g(y) = z$. With f onto and $y \in B$, there exists $x \in A$ with $f(x) = y$. Hence, $z = g(y) = g(f(x)) = (g \circ f)(x)$, so the range of $g \circ f = C =$ the codomain of $g \circ f$, and $g \circ f$ is onto.

□

Function composition is not commutative, but it is associative.

6.4.2 Collection of functions

If A is a set then

$$A^A = \{f \mid f : A \to A\}$$

is the collection of functions $A \to A$. So the function composition is a binary operation on A^A.

6.4.3 Theorem

If $f : A \to B, g : B \to C$, and $h : C \to D$, then

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

Proof. We have

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

and

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

Therefore, we have $(h \circ g) \circ f = h \circ (g \circ f)$. □

6.4.4 Powers of functions

If $f : A \to A$, we define $f^1 = 1$, and for $n \in \mathbb{Z}^+, f^{n+1} = f \circ f(^n)$.

This definition is another example wherein the result is defined *recursively.* With $f^{n+1} = f \circ (f^n)$, we see the dependence of f^{n+1} on a previous power, namely, f^n.

6.5 Invertible functions

6.5.1 Converse of a relation

For sets A, B, if R is a relation from A to B, then the *converse* of R, denoted R^c, is the relation from B to A defined by

$$R^c = \{(b, a) \mid (a, b) \in R\}.$$

We simply interchange the components of each ordered pair in R.

6.5.2 Invertible function

If $f : A \to B$, then f is said to be *invertible* if there is a function $g : B \to A$ such that $g \circ f = 1_A$ and $f \circ g = 1_B$.

6.5.3 Uniqueness

If a function $f : A \to B$ is invertible and a function $g : B \to A$ satisfies $g \circ f = 1_A$ and $f \circ g = 1_B$, then this function g is unique.

Proof. If g is not unique, then there is another function $h : B \to A$ with $h \circ f = 1_A$ and $f \circ h = 1_B$. Consequently,

$$h = h \circ 1_B = h \circ (f \circ g) = (h \circ f) \circ g = 1_A \circ g = g.$$

□

As a result of this theorem, we shall call the function g the inverse of f and shall adopt the notation $g = f^{-1}$. Note that $f^{-1} = f^c$ and $(f^{-1})^{-1} = f$.

6.5.4 Theorem

$f : A \to B$ is invertible if and only if f is bijective.

Proof. Assuming that f is invertible, we have a unique function $g : B \to A$ with $g \circ f = 1_A, f \circ g = 1_B$. If $a_1, a_2 \in A$ with $f(a_1) = f(a_2)$, then $g(f(a_1)) = g(f(a_2))$. It follows that $a_1 = a_2$, so f is one-to-one. For the onto property, let $b \in B$, then $g(b) \in A$. We have $b = 1_B(b) = (f \circ g)(b) = f(g(b))$, so f is onto.

For the other direction, suppose $f : A \to B$ is bijective. Since f is onto, for each $b \in B$, there is an $a \in A$ with $f(a) = b$. Consequently, we define the function $g : B \to A$ by $g(b) = a$, where $f(a) = b$. Our definition of g such that $g \circ f = 1_A$ and $f \circ g = 1_B$, so we find that f is invertible, with $g = f^{-1}$. $\square$

6.5.5 Theorem

If $f : A \to B, g : B \to C$ are invertible functions, then $g \circ f : A \to C$ is invertible and

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

6.6 Inverse image

If $f : A \to B$ and $B_1 \subseteq B$, then $f^{-1}(B_1) = \{x \in A \mid f(x) \in B_1\}$. The set $f^{-1}(B_1)$ is called the *preimage or inverse image* of B_1 under f.

Note. $f^{-1}(B_1)$ is defined even if f is not invertible.

6.6.1 Examples

- For $f : \mathbb{Z} \to \mathbb{Z}$, we have

$$f^{-1}[\{2\}] = \{2\}.$$

- For $f : \mathbb{Z} \to \mathbb{Z}$, we have

$$f^{-1}[\{0\}] = \{x \in \mathbb{Z} \mid f(x) \in \{0\}\} = \{x \in \mathbb{Z} \mid f(x) = 0\}$$

  and

$$f^{-1}[\{1, 2\}] = \varnothing.$$

- For $f : \mathbb{Z} \to \mathbb{Z}_2$, we have

$$f^{-1}[\{0\}] = 2\mathbb{Z} \qquad \text{even integers}$$

  and

$$f^{-1}[\{1\}] = 2\mathbb{Z} + 1 \qquad \text{odd integers}$$

6.7 Theorem

If $f : A \to B$ and $B_1, B_2 \subseteq B$, then

(a) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$;

(b) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$;

(c) $f^{-1}(\overline{B_1}) = \overline{f^{-1}(B_1)}$.

6.8 Finite sets

Let $f : A \to B$ for finite sets A and B, where $|A| = |B|$. Then the following statements are equivalence: (a) f is one-to-one; (b) f is onto; and (c) f is invertible.