Abstract Algebra Lecture Notes

Review: Handout on Writing Proofs

Review Herstein, Chapter 1

Section 1.1: Intro

Section 1.2: Set Theory

Section 1.3: Functions
(Some notes on following pages)

Section 1.4: A(S) will be discussed in class

Section 1.5: The Integers

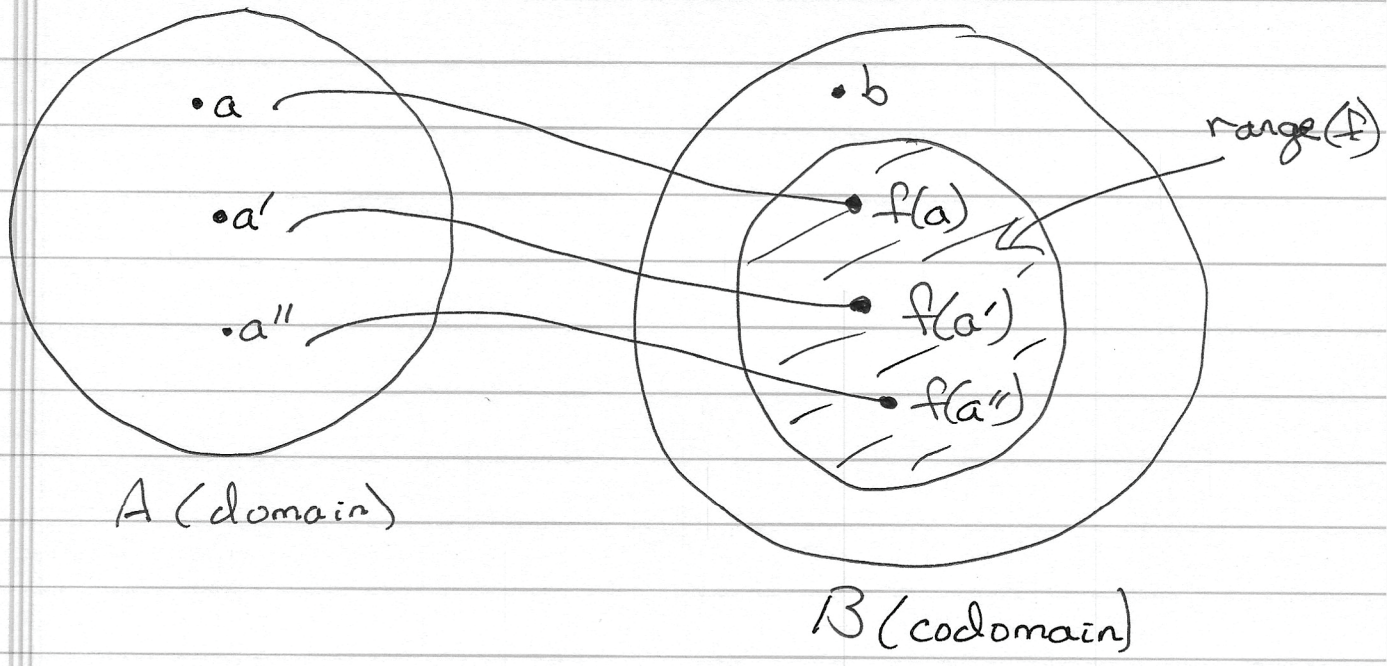
1.3 Review

Functions = Mappings

The informal definition of a function f from a set A to a set B is that it is a rule that assigns to each element $a \in A$ a single value $f(a) \in B$. We write

$$f : A \to B$$

to denote that f is a function from A to B.



Each $a \in A$ is assigned <u>one</u> value $f(a) \in B$.
It's OK if $f(a) = f(a')$ for some $a \neq a'$.
Not every $b \in B$ need equal an $f(a)$

The <u>domain</u> of f is A.

The <u>codomain</u> or <u>target</u> of f is B

The image of $a \in A$ is $f(a)$

The range of f is

$$\text{range}(f) = \{f(a) : a \in A\}$$

Thus the range is the set of all possible images $f(a)$ over all $a \in A$.

Precise Definition

A function $f: A \to B$ is the set of ordered pairs $\{(a, f(a)) : a \in A\}$

For each $a \in A$, there is only one ordered pair (a, b) whose first coordinate is a, and it is the one with $b = f(a)$.

Equality

Two functions f & g are equal if they have the same domain A, the same codomain B, and $f(a) = g(a)$ for every $a \in A$.

In this case we write $f = g$.

Definition

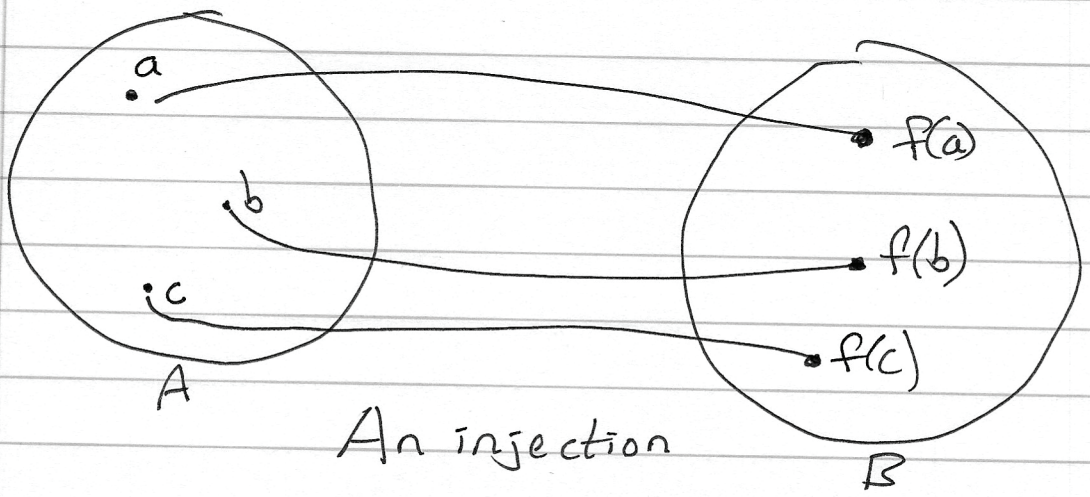
A function $f: A \to B$ is injective or one-to-one (written 1-1) if

$$a \neq b \implies f(a) \neq f(b).$$

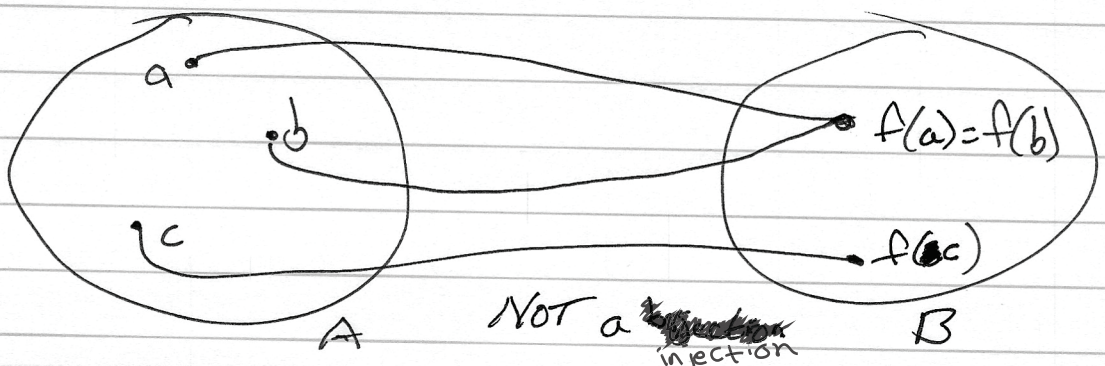
The CONTRAPOSITIVE FORM is equivalent and usually easier to use in practice:

$$f(a) = f(b) \implies a = b$$

For a 1-1 function, each $a \in A$ maps to a unique $f(a)$ in B.



An injection

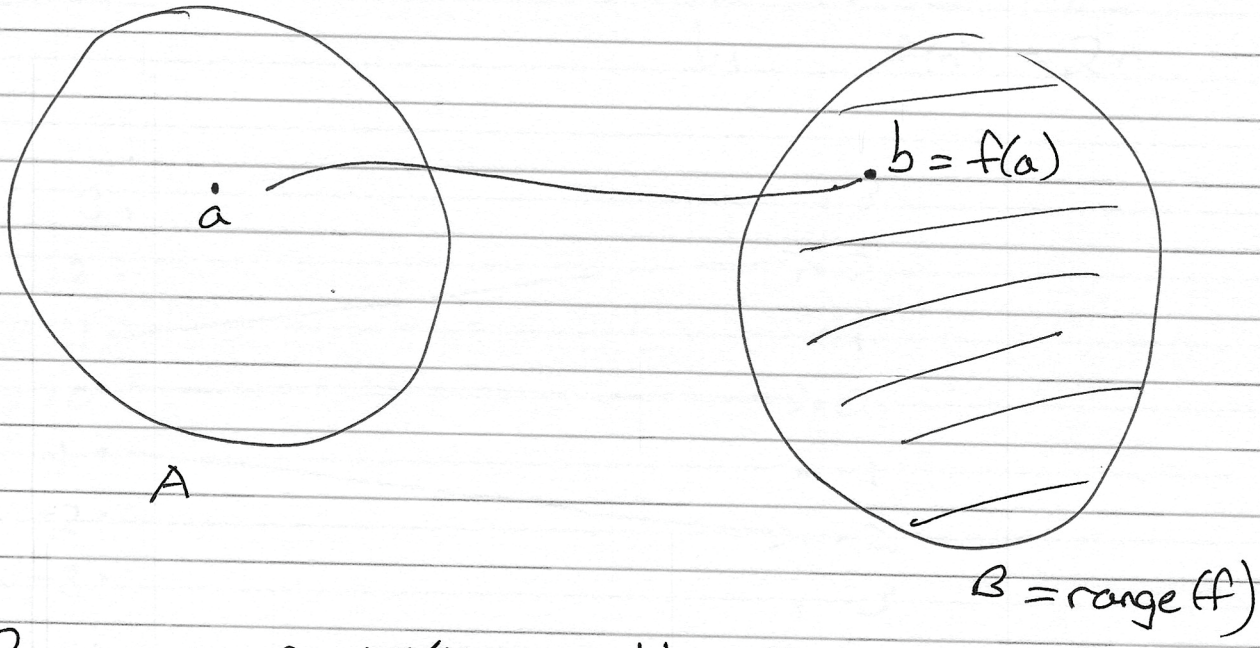


NOT a injection

Definition

$f: A \to B$ is surjective or onto if the range(f) is all of B:

$$\text{range}(f) = B.$$



B is onto if $\forall b \in B$,
$\exists a \in A$ such that $f(a) = b$.
(There could be more than one a that maps to b.)

Definition

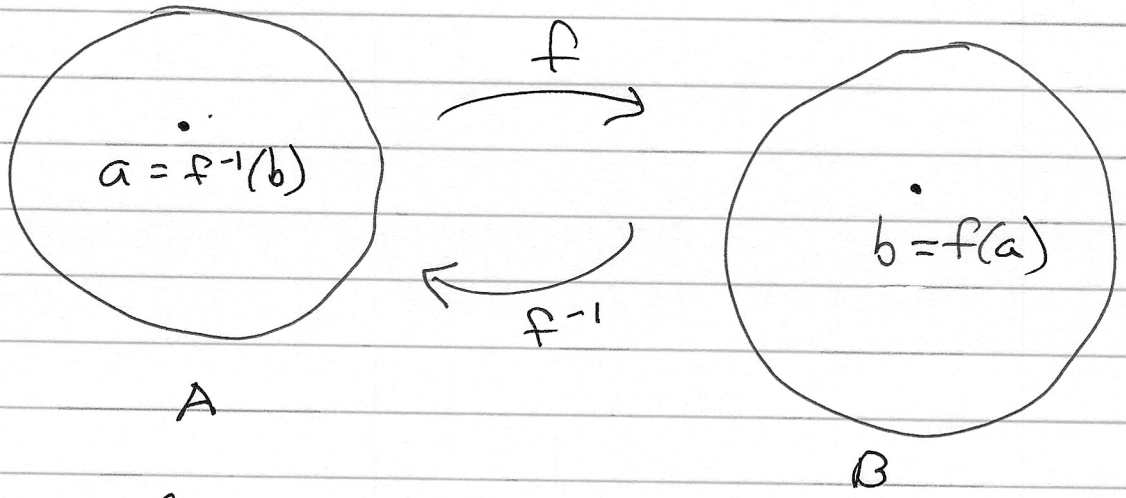
$f: A \to B$ is a bijection or 1-1 correspondence if it is both 1-1 & onto.

This means that $\forall b \in B$ there is a unique $a \in A$ such that $f(a) = b$.

Definition

If $f: A \to B$ is a bijection then there is an inverse function $f^{-1}: B \to A$ defined by

$$f^{-1}(b) = a \quad \text{if } f(a) = b$$



Example

The inverse function of $f: \mathbb{R} \to \mathbb{R}$, $f(x) = 2x$ is $f^{-1}: \mathbb{R} \to \mathbb{R}$, $f^{-1}(y) = y/2$

Example

The identity function on a set A is

$$i: A \to A$$
$$i(x) = x$$

This is a bijection, & $i^{-1} = i$.

The letter e is often used instead of i.

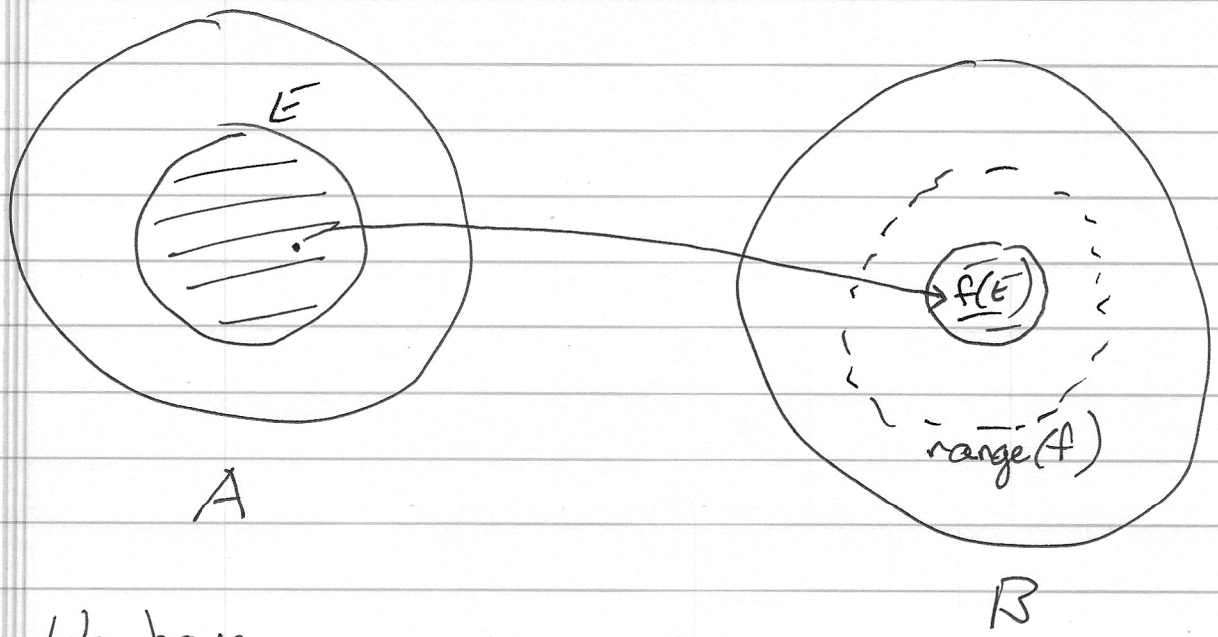
Direct Image

Let $f: A \to B$ be a function. The direct image of $E \subseteq A$ is

$$f(E) = \{f(a) : a \in E\}$$

↑

We are declaring what f of a set means



We have

$$f(E) \subseteq \text{range}(f) = \{f(a) : a \in A\} = f(A)$$

Example $f: \mathbb{R} \to \mathbb{R}$
$f(x) = 2x$

If $E = [2,3]$ then $f(E) = \{f(x) : x \in [2,3]\}$
$= \{2x : 2 \leq x \leq 3\}$
$= [4,6]$

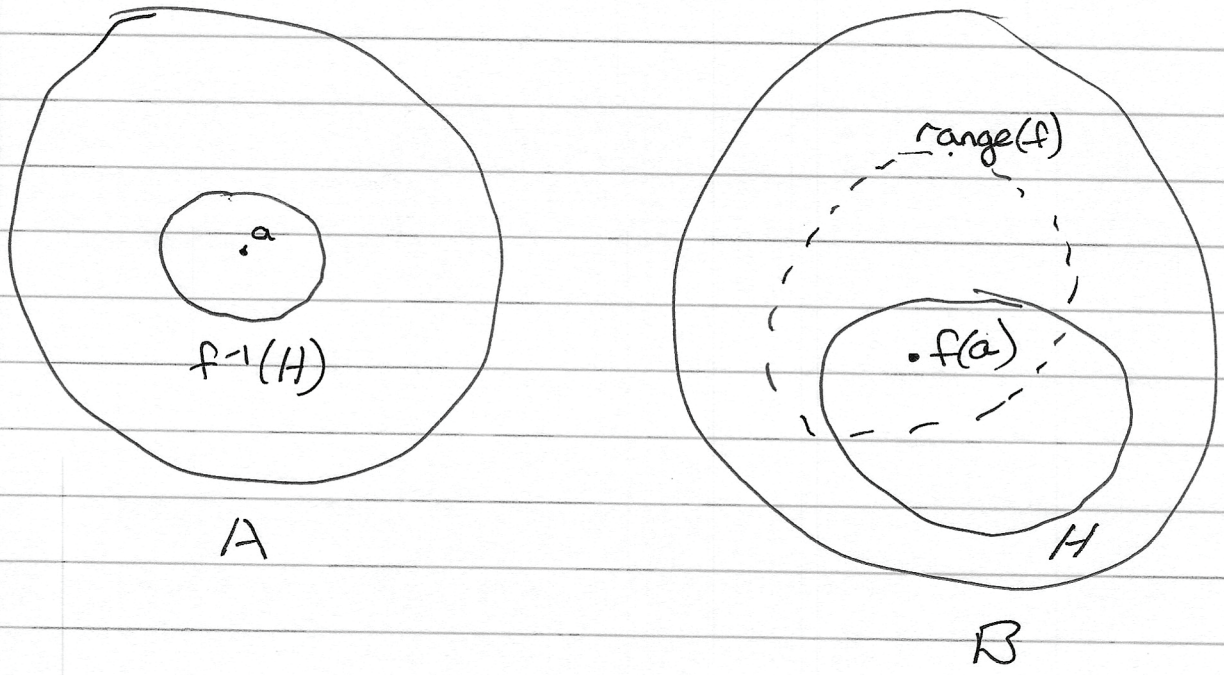
Preimage = Inverse Image

Let $f: A \to B$ be a function. The preimage or inverse image of $H \subseteq B$ is

$$f^{-1}(H) = \{a \in A : f(a) \in H\}$$

NOTE: f^{-1} here is not the inverse function! f need not be a bijection, there might not even be an inverse function.

We use context here: If H is a set then $f^{-1}(H)$ means the inverse image of H.



If $H \cap \text{range}(f) = \emptyset$ then $f^{-1}(H) = \emptyset$, even if H is nonempty.

Example $f: \mathbb{Z} \to \mathbb{Z}$

$f(n) = 2n$

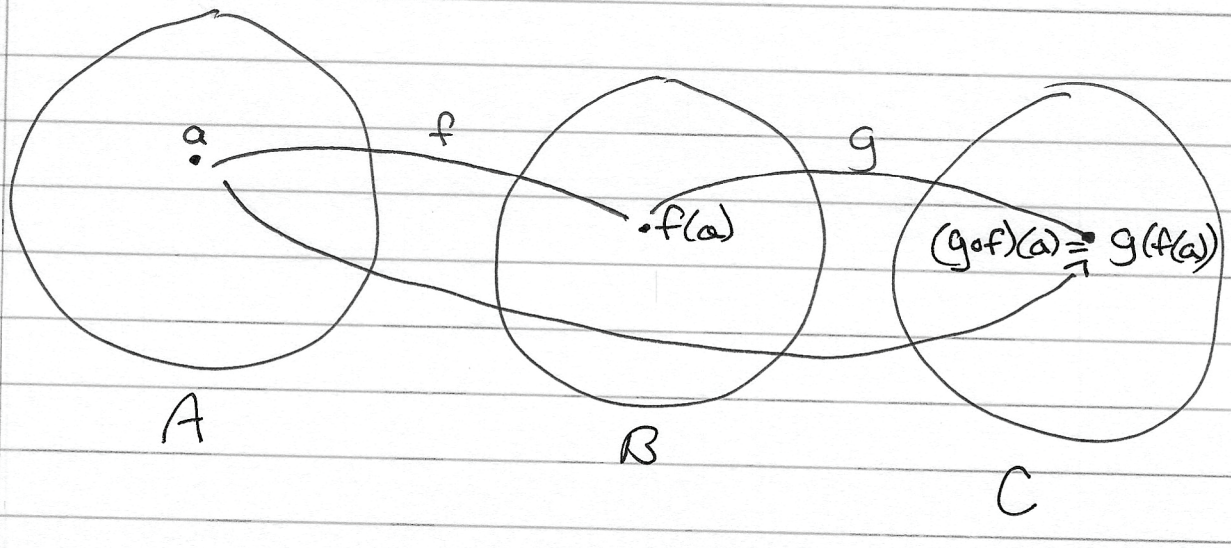
If $H = \{7, 8, 9, 10\}$ then $f^{-1}(H) = \{4, 5\}$

because $f(4) = 8 \in H$ & $f(5) = 10 \in H$
and no other integers n map into H.

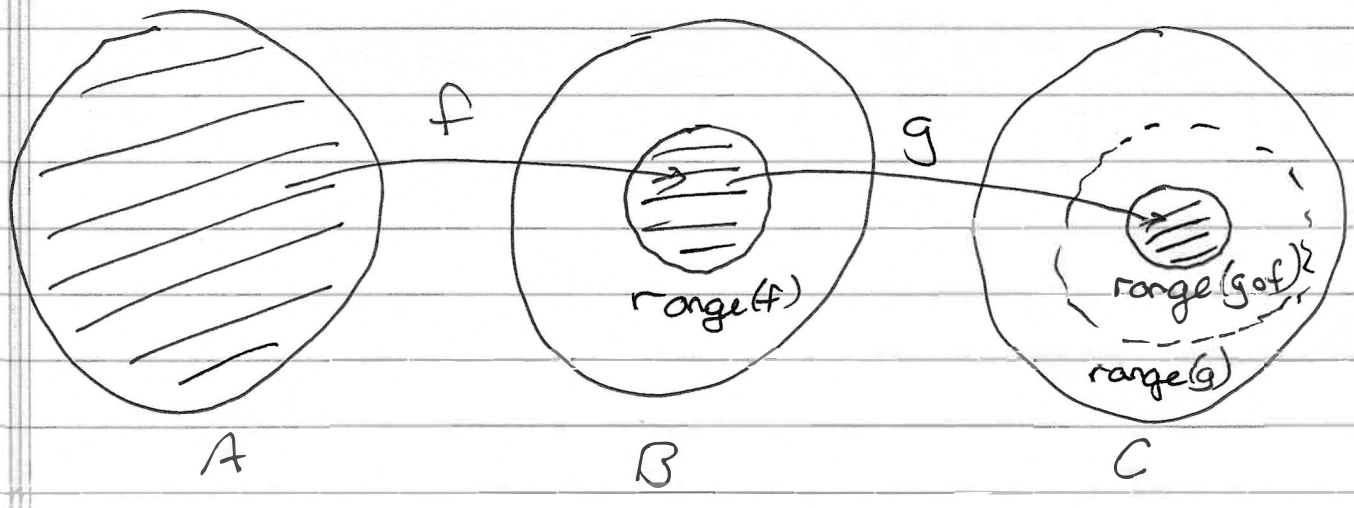
Composition

The composition of $f: A \to B$ with $g: B \to C$ is the function $g \circ f: A \to C$ defined by

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



We have $\text{range}(g \circ f) \subseteq \text{range}(g)$, but equality need not hold.



Theorem
Composition of functions is associative.
That is, if

$$f: A \to B, \quad g: B \to C, \quad h: C \to D$$

then

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

Proof:
If $x \in A$ then

$$\begin{aligned}(h \circ (g \circ f))(x) &= h((g \circ f)(x)) \\ &= h(g(f(x))) \\ &= (h \circ g)(f(x)) \\ &= ((h \circ g) \circ f)(x)\end{aligned}$$

→

Since $(h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)$ for every $x \in A$, we conclude that $h \circ (g \circ f)$ and $(h \circ g) \circ f)$ are the same function. ∎

Now that we've proved that composition of functions is associative, we never need to prove it again.

NOTE: In general $f \circ g \neq g \circ f$!

(In general means that it can happen for some functions f & g, but not all).

Example: Define $f, g : \mathbb{R} \to \mathbb{R}$ by $f(x) = x+1$ & $g(x) = x^2$. Then check that $g \circ f \neq f \circ g$

Exercise Prove that

(a) $f: A \to B$ & $g: B \to C$ both injective $\Rightarrow$ $g \circ f$ injective

(b) $f: A \to B$ & $g: B \to C$ both surjective $\Rightarrow$ $g \circ f$ surjective

(c) $f: A \to B$ & $g: B \to C$ both bijections $\Rightarrow$ $g \circ f$ bijective

(Recall injective = 1-1 & surjective = onto)

Exercise Let $f: A \to B$ & $g: B \to C$ be functions. Prove that:

(a) $g \circ f$ injective $\Longrightarrow$ f injective

(b) $g \circ f$ surjective $\Longrightarrow$ g surjective

Give examples of functions f & g such that

(c) $g \circ f$ is injective but g is not injective

(d) $g \circ f$ is surjective but f is not surjective

Exercise Let $f: A \to A$ be a bijection and let $i_A: A \to A$ be the identity function on A, and $i_B: B \to B$ the identity function on B. Prove that

$$f \circ f^{-1} = i_B \quad \& \quad f^{-1} \circ f = i_A$$

Give examples of functions $f: A \to B$ & $g: B \to A$ such that

$$g \circ f = i_A \text{ but } f \circ g \neq i_B$$

1.5 The Integers (Review)

Review the basic properties of

the natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$
the integers $\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$

Well-ordering Principle

Every nonempty set of nonnegative integers has a smallest element.

Euclidean Algorithm

If $m, n \in \mathbb{Z}$, $n > 0$, then $\exists\, q, r \in \mathbb{Z}$ with $0 \leq r < n$ s.t.

$$m = qn + r$$

Fundamental Theorem of Arithmetic
= unique factorization of positive integers as product of primes.

1.6 Induction

Review induction.