WINTER 2023 EDITION
(W/ LACZKOVICH-SÓS)

REAL ANALYSIS I - MATH 2122B

I. LOGIC & PROOF (cf. sections 2.2, 2.3)

1. LOGICAL CONNECTIVES

statement = a sentence that can be classified (determined) as true or false.

E.g. "$2+2=4$" has truth value T
"Every positive real number is greater than 1" has truth value F
But "How are you?", "This sentence is false" are not statements.

Basic logical connectives:

NAME	SYMBOL	USED	READ
negation	$\neg$	$\neg p$	not p
conjunction	$\wedge$	$p \wedge q$	p and q
disjunction	$\vee$	$p \vee q$	p or q
implication	$\Rightarrow$	$p \Rightarrow q$	if p, then q
equivalence	$\Leftrightarrow$	$p \Leftrightarrow q$	p if and only if q

We define the above by their truth tables, as follows:

p	$\neg p$
T	F
F	T

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

p	q	$p \Leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

A compound statement whose truth value is always T is called a tautology.

E.g. $[(p \Rightarrow q) \wedge (q \Rightarrow p)] \Leftrightarrow (p \Leftrightarrow q)$ is a tautology.

Check:

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$(p \Rightarrow q) \wedge (q \Rightarrow p)$	$p \Leftrightarrow q$	LHS $\Leftrightarrow$ RHS
T	T	T	T	T	T	T
T	F	F	T	F	F	T
F	T	T	F	F	F	T
F	F	T	T	T	T	T

✓

Other examples of commonly used tautologies:

1) $(p \vee q) \vee r \iff p \vee (q \vee r)$
$(p \wedge q) \wedge r \iff p \wedge (q \wedge r)$ } associativity

2) $p \vee q \iff q \vee p$
$p \wedge q \iff q \wedge p$ } commutativity

3) $p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r)$
$p \vee (q \wedge r) \iff (p \vee q) \wedge (p \vee r)$ } distributive laws

4) $\neg(p \vee q) \iff (\neg p) \wedge (\neg q)$
$\neg(p \wedge q) \iff (\neg p) \vee (\neg q)$ } de Morgan laws

5) $p \vee \neg p$ "tertium non datur"

6) $[\neg(p \Rightarrow q)] \iff (p \wedge \neg q)$.

7) $\neg(\neg p) \iff p$.

The opposite of tautology = contradiction = a logical sentence which is always false.

E.g., "$p \wedge \neg p$" is false, independently of the truth value of p.

The logical square of implications:

simple statement $p \Rightarrow q$	converse st't $q \Rightarrow p$
inverse st't $\neg p \Rightarrow \neg q$	contrapositive st't $\neg q \Rightarrow \neg p$

2. QUANTIFIERS

predicate = a sentence whose truth value depends on a parameter (variable)

E.g., "$x^2 + 2x + 1 = 0$".

Quantifiers make predicates into statements.

$\forall$ = universal quantifier = "for all"

$\exists$ = existential quantifier = "there exists"

E.g., "$\forall x \in \mathbb{R}$, $x^2+2x+1=0$" has truth value F
"$\exists x<0$ s.t. $x^2+2x+1=0$" has truth value T.

Warning: If a quantifier is not specified, the universal quantifier is assumed!
E.g., "If $x>2$, then $x^2>4$" means "$\forall x \in \mathbb{R}$, $x>2 \Rightarrow x^2>4$"

The order of quantifiers matters!
E.g., "$\forall x \in (0,\infty)\ \exists n \in \mathbb{N}$ s.t. $\frac{1}{n}<x$" (called Archimedean Principle")
is not equivalent to "$\exists n \in \mathbb{N}\ \forall x \in (0,\infty)$, $\frac{1}{n}<x$" (which is false!)

In general:

$$\exists x\ \forall y,\ p(x,y) \quad \underset{\not\Leftarrow}{\Rightarrow} \quad \forall y\ \exists x \text{ s.t. } p(x,y)$$

However, $\exists x\ \exists y \Leftrightarrow \exists y\ \exists x$ and $\forall x\ \forall y \Leftrightarrow \forall y\ \forall x$.

Negating quantifiers: $\neg(\forall x, p(x)) :\Leftrightarrow \exists x$ s.t. $\neg p(x)$
$\neg(\exists x$ s.t. $p(x)) :\Leftrightarrow \forall x, \neg p(x)$.

3. TECHNIQUES OF PROOF

proof = verification that a given claim is a tautology.

Until proven, a statement is a conjecture (or a hypothesis).
Examples of conjectures:
C.1. For all $n \in \mathbb{N}$, n^2+n+11 is a prime number.
C.2 (Goldbach Conjecture) For all n even and greater than 2, there exist primes p_1, p_2 such that $n = p_1 + p_2$.

Naive inductive reasoning: "proving" C.1. We check that for
$n=0$, $n^2+n+11 = 11$ is prime,
$n=1$, $n^2+n+11 = 13$ is prime,
$n=2$, $n^2+n+11 = 17$ is prime,
$n=3$, $n^2+n+11 = 23$ is prime,
$n=4$, $n^2+n+11 = 31$ is prime ..., so we expect it works for all n.
Drawing this conclusion is an example of inductive reasoning.

In fact, this expectation is false. For instance, when $n=11$, then $n^2+n+11=(11+1+1)\cdot 11=13\cdot 11$ is not prime. This is a counterexample.

Correct inductive reasoning is based on:

Principle of Mathematical Induction. Let $P(n)$ be a statement with parameter $n\in\mathbb{N}$, and let $n_0\in\mathbb{N}$ be given.
If $P(n_0)$ is true, and, for all $k\geq n_0$, $P(k)$ true implies $P(k+1)$ true, then $P(n)$ is true for all $n\geq n_0$.

Example: Show that $1+2+\ldots+n=\frac{n(n+1)}{2}$ for all $n\in\mathbb{N}_+$.
Proof by Induction:
Step 1: Verify for $n=1$. $LHS(1)=1$, $RHS(1)=\frac{1\cdot(1+1)}{2}=1$, so $LHS(1)=RHS(1)$ ✓
Step 2 (aka Inductive Step):
Suppose $k\geq 1$ and the claim holds true for k. We want to show that it also holds for $k+1$.

$$LHS(k+1)=1+2+\ldots+k+(k+1)\overset{\text{by Inductive Hypothesis}}{=}\frac{k(k+1)}{2}+(k+1)=\frac{(k+1)(k+2)}{2}$$

But $\frac{(k+1)(k+2)}{2}=\frac{(k+1)((k+1)+1)}{2}=RHS(k+1)$, so the claim is proved.

Thus, by the Principle of Math Induction, given equality holds for all $n\geq 1$. ■

More Examples: Prove that
- $\forall n\in\mathbb{N}_+$, $2^n>n$ (Thm. 2.4)
- If $a>-1$, then $\forall n\in\mathbb{N}_+$, $(1+a)^n\geq 1+na$, with equality only if $n=1 \vee a=0$. (Bernoulli's Ineq., Thm. 2.5)

Exercise: Find a mistake in the following "proof".
Claim 1: All cats are black.
Pf. It follows from the fact that there is a black cat and the next claim. □
Claim 2: All cats are of the same color.
Pf. We'll prove, by induction on n, that $P(n)=\{$all n-element sets of cats are of the same color$\}$ holds for all $n\geq 1$.
Step 1. Trivial. ✓ Step 2. Given a collection of $k+1$ cats

k of the same color   k of the same color

, since the cats in the overlaps have a fixed color, the claim follows. ■

<u>Deductive</u> reasoning: Building a sequence of implications $p_1 \Rightarrow p_2$, $p_2 \Rightarrow p_3, \ldots, p_k \Rightarrow p_{k+1}$, and applying the <u>transitivity</u> tautology

$$[(p_1 \Rightarrow p_2) \wedge (p_2 \Rightarrow p_3) \wedge \ldots \wedge (p_k \Rightarrow p_{k+1})] \Rightarrow (p_1 \Rightarrow p_{k+1}).$$

We deduce from:
1) axioms
2) definitions
3) theorems already established
4) logical implications of 1), 2), 3).

<u>Example.</u>

Prove that the function $f(x) = x^2 - 4$ is continuous at $c = 1$.

We want to show that: $\forall \varepsilon > 0\ \exists \delta > 0\ \forall x \in \mathbb{R},\ |x-c| < \delta \Rightarrow |f(x) - f(c)| < \varepsilon$; i.e,
$\forall \varepsilon > 0\ \exists \delta > 0\ \forall x \in \mathbb{R},\ |x-1| < \delta \Rightarrow |(x^2-4) - (-3)| < \varepsilon$.

Begin with <u>Heuristic</u>: "What does it entail for $|(x^2-4)-(-3)|$ to be less than ε?"

Notice that $(x^2-4)-(-3) = x^2 - 1 = (x-1)(x+1)$, and hence, if $|x-1| < \delta$, then $|(x^2-4)-(-3)| = |(x-1)\cdot(x+1)| = |x-1| \cdot |x+1| < \delta \cdot |x+1|$.

We thus need to find an upper bound for $|x+1|$. As $\delta > 0$ may be chosen as small as we wish, we may assume that $\delta \leq \frac{1}{2}$. Then, $|x-1| < \delta$ implies that $1 - \frac{1}{2} < x < 1 + \frac{1}{2}$, or $\frac{1}{2} < x < \frac{3}{2}$, and hence $\frac{3}{2} < x+1 < \frac{5}{2}$.

To sum up, by requiring that $\delta \leq \frac{1}{2}$, we get that $|x-1| < \delta$ implies $|(x^2-4)-(-3)| = |x-1| \cdot |x+1| < \delta \cdot \frac{5}{2}$.

Since we want $|x-1| \cdot |x+1|$ less than ε, it thus suffices to choose a δ such that $\delta \cdot \frac{5}{2} < \varepsilon$. Indeed, $[(|x-1| \cdot |x+1| < \frac{5\delta}{2}) \wedge (\frac{5\delta}{2} < \varepsilon)] \Rightarrow |x^2-1| < \varepsilon$.

For instance, $\frac{\varepsilon}{3}$ has this property, i.e., $\frac{\varepsilon}{3} \cdot \frac{5}{2} = \frac{5}{6}\varepsilon < \varepsilon$.

We have thus shown that, if $\delta = \min\{\frac{1}{2}, \frac{\varepsilon}{3}\}$, then $\frac{5\delta}{2} < \varepsilon$ and $|x+1| < \frac{5}{2}$. We are finally ready do give a proof of the claim:

<u>Proof</u>: Let $\varepsilon > 0$ be arbitrary. Choose $\delta = \min\{\frac{1}{2}, \frac{\varepsilon}{3}\}$.

Then, for every $x \in \mathbb{R}$, $|x-1| < \delta \Rightarrow |(x^2-4)-(-3)| = |x-1| \cdot |x+1| < \frac{5}{2}\delta \leq$

$\leq \frac{5}{2} \cdot \frac{\varepsilon}{3} = \frac{5\varepsilon}{6} < \varepsilon$, as required. ∎

Proof by Contradiction:

For claims in the form of a single compound statement p, use the tautology

$$[(\neg p) \Rightarrow \text{contr.}] \Rightarrow p.$$

For claims in the form of an implication $p \Rightarrow q$, use the tautology

$$(p \Rightarrow q) \Leftrightarrow [(p \wedge \neg q) \Rightarrow \text{contr.}].$$

Examples:

1) Claim: $\sqrt{2}$ is not a rational number.

Pf. (by Contradiction) Suppose to the contrary that $\sqrt{2}$ is a rational number. Then, one can write $\sqrt{2} = a/b$, for some $a, b \in \mathbb{N}_+$, where a, b have no common factors (i.e., a, b are "in lowest terms"). Squaring both sides of this equation, one gets $2 = a^2/b^2$, hence $a^2 = 2 \cdot b^2$, which proves that a^2 is even. It follows that a is even (indeed, for else $a = 2l+1$ and so $a^2 = 4l^2 + 4l + 1 = 2(2l^2 + 2l) + 1$ is odd as well), hence $a = 2k$ for some $k \in \mathbb{N}_+$. Then, $a^2 = 2b^2$ gives $4k^2 = 2b^2$, or $b^2 = 2k^2$, which means that b^2 is even. Thus, again, b is even, or $b = 2l$ for some $l \in \mathbb{N}_+$. We thus obtained that both a and b are divisible by 2, which in conjunction with the assumption that they be in lowest terms is a contradiction. This completes the proof. ∎

2) Claim. If $5m$ is odd, then so is m.

Here, we have $p = \{5m \text{ is odd}\}$, $q = \{m \text{ is odd}\}$, and the Claim is "$p \Rightarrow q$".

Pf. (by Contradiction):

For a proof by contradiction, suppose that $5m$ is odd (p) and m is even ($\neg q$). Then, one can write $m = 2k$ for some $k \in \mathbb{N}$. It follows that $5m = 5 \cdot 2k = 2 \cdot (5k)$ is even. In conjunction with the assumption that $5m$ odd, this is a contradiction. This proves that m is odd. ∎

Proof by Passing to Contrapositive:

For claims of the form "$p \Rightarrow q$", use the equivalence of it with "$\neg q \Rightarrow \neg p$".

Examples: 1) Claim. If $5m$ is odd, then so is m.

Here, again, $p = \{5m \text{ is odd}\}$, $q = \{m \text{ is odd}\}$, hence $\neg p = \{5m \text{ is even}\}$ and $\neg q = \{m \text{ is even}\}$.

Pf. Suppose that m is even. Then, one can write $m = 2k$ for some $k \in \mathbb{Z}$. It follows that $5m = 5 \cdot 2k = 2 \cdot (5k)$ is also even, which completes the proof. ∎

2) Claim. Let $f : [0,1] \to \mathbb{R}$ be an integrable function. If $\int_0^1 f(x)\,dx \neq 0$, then there exists $x_0 \in [0,1]$ s.t. $f(x_0) \neq 0$.

Here, $p = \{\int_0^1 f(x)\,dx \neq 0\}$, $q = \{\exists x_0 \in [0,1] \text{ s.t. } f(x_0) \neq 0\}$, so $\neg q = \{\forall x \in [0,1],\ f(x) = 0\}$ (recall negation of quantifiers!) and $\neg p = \{\int_0^1 f(x)\,dx = 0\}$.

Pf: Suppose that, for all $x \in [0,1]$, $f(x) = 0$. Then, f is a constant 0 function, and so by definition of Riemann integral,

$$\int_0^1 f(x)\,dx = \underbrace{(1-0)}_{\text{endpoints}} \cdot \underbrace{0}_{\text{value of the constant function}} = 0.$$

This completes the proof. ∎

II. SETS & FUNCTIONS (cf. 2.4)

1. BASIC SET OPERATIONS

The notion of *set* is *undefinable*, like that of a point or an infinite straight line. We can nonetheless define every specific set A by assuming the following

Axiom: For all x, either $x \in A$ or else $x \notin A$ (meaning $\neg(x \in A)$) is a statement.

If $x \in A$, then x is called an *element of A*.

Two typical ways of defining sets:

- by specifying their elements $A = \{1,2,3,4,5\}$
- as a subset of some known set $A = \{x \in \mathbb{N} \mid 0 < x \le 5\}$.

Def. We say that B is a <u>subset</u> of a set A (or, that B is <u>contained in</u> A), when every element of B is an element of A; i.e, $\forall x,\ x \in B \Rightarrow x \in A$.
We write $B \subset A$ (or $B \subseteq A$). If $B \subset A \wedge \neg(A \subset B)$, we say B is a proper subset of A, and write $B \subsetneq A$.

<u>Remark</u>. If A is a set, $p(x)$ a predicate, then defining $B = \{x \in A : p(x)\}$ produces a set (that is, the preceding Axiom is satisfied by B).

<u>Def.</u> We say that set A, B are <u>equal</u>, written $A = B$, when $A \subset B \wedge B \subset A$ (equivalently, when $\forall x,\ x \in A \Leftrightarrow x \in B$).

<u>Warning</u>: To properly define a set, it's best to define it as a subset of some universal set.
E.g, $A = \{x \in \mathbb{R} : x^2 < 1\}$ or $B = \{n \in \mathbb{N} : \exists m \in \mathbb{N} \text{ s.t. } n = m^2\}$, but not $A = \{x : x \geq 0\}$, b/c it is not known what x can be (a real number, an animal, a date?)

<u>Example</u> of an improper set declaration – <u>Russel's Paradox</u>:

$$A := \{x \mid x \notin x\}.$$

Claim: A is <u>not</u> a set! Indeed, if it were then we'd have $A \in A$ or else $A \notin A$, but both these statements lead to a contradiction (by def'n of A). □

<u>Example</u>: The "set of all sets" is also <u>not</u> a set – proof later.

<u>Question</u>: How do we even know if there are any sets???

<u>Answer</u>: There exists an <u>empty set</u>; i.e, a set with no elements.

<u>Def</u>. The <u>empty set</u> is defined as $\emptyset = \{x : x \neq x\}$. (Equivalently, $\forall x, x \notin \emptyset$.)

More good news: The entire mathematics can be constructed from this single set!

<u>Thm</u>. Let A be any set. Then, $\emptyset \subset A$.

Pf. We want to show that $p = \{\forall x,\ x \in \emptyset \Rightarrow x \in A\}$ is a tautology. For a proof by contradiction, suppose $\neg p$; i.e, suppose that $\exists x$ s.t. $x \in \emptyset \wedge x \notin A$. The latter implies that $\exists x$ s.t. $x \in \emptyset$, which contradicts definition of $\emptyset$. Thus, $\emptyset \subset A$. ∎

Def. Given a set A, its power set is $\mathcal{P}(A) := \{B : B \subset A\}$.

Def. Let A, B be sets. We define
- union of A and B as $A \cup B := \{x : x \in A \vee x \in B\}$
- intersection of A and B as $A \cap B := \{x : x \in A \wedge x \in B\}$
- (set theoretical) difference $A \setminus B := \{x : x \in A \wedge x \notin B\}$.

When $A \cap B = \emptyset$, we say that A and B are disjoint.

When A is a subset of some universal set U, then $U \setminus A$ is called the complement of A (in U) and denoted A^c.

Thm. Let A, B, C be subsets of a universal set U. Then

(i) $(A^c)^c = A$

(ii) $A \cup A^c = U$

(iii) $A \cap A^c = \emptyset$

(iv) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ } distributive laws

(v) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(vi) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ } de Morgan laws

(vii) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

More (obvious) properties: $A \setminus A = \emptyset$; $A \setminus \emptyset = A$; $A \cap A = A$; $A \cup A = A$; $A \cup B = B \cup A$; $A \cap B = B \cap A$; $A \subset A$; $A \subset B \wedge B \subset C \Rightarrow A \subset C$.

2. RELATIONS

Def. An ordered pair (of elements a, b) is defined as

$$(a, b) := \{\{a\}, \{a, b\}\}.$$

Remark: The above definition allows us to distinguish between the first and the second element of a pair (hence, the name "ordered"). For example, $(1,2) \neq (2,1)$. Indeed, the two-element set $(1,2)$ contains the singleton $\{1\}$, which is not an element of $(2,1) = \{\{2\}, \{2,1\}\}$.

Thm. $(a, b) = (c, d)$ iff $[a = c \wedge b = d]$.

Pf. ($\Leftarrow$) Suppose $a = c \wedge b = d$. Then, $\{a\} = \{c\}$ and $\{a, b\} = \{c, d\}$, so $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. ✓

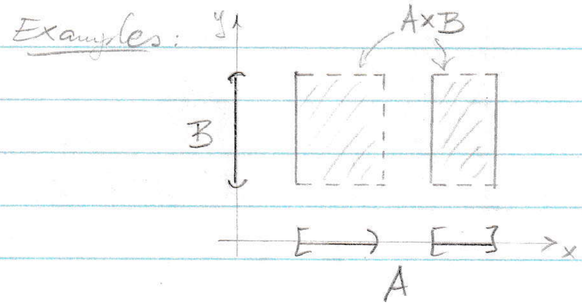
($\Rightarrow$) Suppose conversely that $(a,b)=(c,d)$; i.e., $\{\{a\},\{a,b\}\}=\{\{c\},\{c,d\}\}$.

Case 1. Suppose $a=b$. Then $\{a,b\}=\{a\}$, and hence $(a,b)=\{\{a\}\}$. Since $\{\{c\},\{c,d\}\}=(c,d)\subset(a,b)=\{\{a\}\}$, it follows that $\{c\}=\{c,d\}$ and $\{c\}=\{a\}$, hence $c=d$ and $c=a$. ✓

Case 2. Suppose finally that $a\neq b$. Then $\{a,b\}\neq\{a\}$, as $\{a,b\}$ is a 2-element set. Now, $\{c\}\in(c,d)=(a,b)=\{\{a\},\{a,b\}\}$ implies $\{c\}=\{a\}\vee\{c\}=\{a,b\}$. The latter is impossible (as $\{a,b\}$ has 2 elements), and so $\{c\}=\{a\}$, hence $c=a$. Similarly, $\{a,b\}\in(a,b)=(c,d)=\{\{c\},\{c,d\}\}$, so $\{a,b\}=\{c\}\vee\{a,b\}=\{c,d\}$. As above, $\{a,b\}=\{c\}$ is impossible, so $\{a,b\}=\{c,d\}$. Thus, $\{c,d\}$ is a 2-element set, hence $c\neq d$. Moreover, as $b\in\{c,d\}$ and $b\neq a=c$, it follows that $b=d$. ∎

Def. Given sets A,B, their Cartesian product $A\times B$ is defined as
$$A\times B=\{(a,b) : a\in A \wedge b\in B\}.$$

Examples:

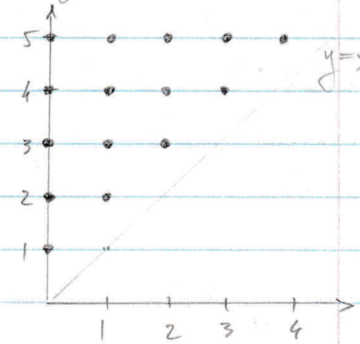


$A=\{1,2,3\}$

$A^2=A\times A=\{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,1),(3,2),(3,3)\}$.

Def. Given sets A,B, a relation between A and B is any subset $R\subset A\times B$. If $(a,b)\in R$, we write aRb and say $a\in A$ and $b\in B$ are related by R. If $B=A$ and $R\subset A\times A$, we say R is a relation on A.

Example: Define $R\subset\mathbb{N}\times\mathbb{N}$ to consist of all pairs of naturals (k,ℓ) that lie above the line $y=x$.



Then, $kR\ell$ iff $k<\ell$.

Thus $R=$ "$<$"

Def. Let A be a set. A relation $R \subset A \times A$ is a <u>partial order</u> relation <u>on</u> A, when

(PO1) $\forall a \in A,\ aRa$ (reflexivity)

(PO2) $\forall a,b \in A,\ (aRb \wedge bRa) \Rightarrow a=b.$

(PO3) $\forall a,b,c \in A,\ (aRb \wedge bRc) \Rightarrow aRc.$ (transitivity)

R is a <u>linear order</u> relation, when it satisfies (PO1)–(PO3) and

(LO) $\forall a,b \in A,\ aRb \vee bRa.$

Examples: 1) $R = "\subset"$ inclusion on $\mathcal{P}(\mathbb{N})$ is a partial order, but not linear order as $\{1\},\{2\}$ are incomparable.

2) $R = "\leq"$ on $\mathbb{N}$ is a linear order

3. FUNCTIONS

Def. Let A, B be sets. A <u>function</u> between A and B is a nonempty relation $f \subset A \times B$ satisfying

$\forall a \in A\ \forall b_1, b_2 \in B,\ ((a,b_1)\in f \wedge (a,b_2)\in f) \Rightarrow b_1 = b_2$ ("vertical line test")

<u>Domain of f</u>: $\mathrm{dom}(f) := \{a \in A : \exists b \in B \text{ s.t. } (a,b)\in f\}$

<u>Range of f</u>: $\mathrm{rng}(f) := \{b \in B : \exists a \in A \text{ s.t. } (a,b)\in f\}.$

The set B is refered to as the <u>codomain</u> of f.

If $\mathrm{dom}(f) = A$, f is called a function <u>from</u> A to B, and we write $f: A \to B$.

When $(x,y)\in f$, we write $y = f(x)$, and call y the <u>image of x</u> under f.

<u>Example</u>. Let U be a universal set, and $A \subset U$.

Define

$$\chi_A : U \to \{0,1\} \text{ as } \chi_A(x) = \begin{cases} 0, & x \in A^c \\ 1, & x \in A \end{cases}.$$

χ_A is called the <u>characteristic function of A</u>.

Def. Let $f: A \to B$ be a function. We say that f is

- <u>surjective</u>, when $\forall b \in B\ \exists a \in A$ s.t. $b = f(a)$ (i.e., $\mathrm{rng}(f) = B$)
- <u>injective</u>, when $\forall a_1, a_2 \in A,\ f(a_1) = f(a_2) \Rightarrow a_1 = a_2$
- <u>bijective</u>, when f is surjective and injective.

<u>Example</u>: $f(x) = x^2$ is surjective onto $[0,+\infty)$ and injective on $[0,+\infty)$.

Functions acting on sets

Def. Let $f: X \to Y$ a function, $A \subset X$, $B \subset Y$. We define

- image of A by f: $f(A) := \{y \in Y;\ \exists a \in A \text{ s.t. } y = f(a)\}$
- inverse image of B by f: $f^{-1}(B) := \{x \in X:\ \exists b \in B \text{ s.t. } f(x) = b\}$.
  (or preimage)

Warning: The symbol "f^{-1}" above should not be mistaken for the inverse function of f, which may not exist.

Thm. Let $f: X \to Y$ be a function, $A, B \subset X$, $E, F \subset Y$. Then,

(i) $A \subset f^{-1}(f(A))$ / inequality: $f(x) = x^2$ on $\mathbb{R}$, $A = [0,1]$ /

(ii) $f(f^{-1}(E)) \subset E$ / inequality: $f: \mathbb{N} \to \mathbb{N}$, $f(k) = 2k$, $E = \{0,1\}$ /

(iii) $f(A \cap B) \subset f(A) \cap f(B)$ / inequality: $f(x) = x^2$, $A = [-1,0]$, $B = [0,1]$ /

(iv) $f(A \cup B) = f(A) \cup f(B)$

(v) $f^{-1}(E \cap F) = f^{-1}(E) \cap f^{-1}(F)$

(vi) $f^{-1}(E \cup F) = f^{-1}(E) \cup f^{-1}(F)$

(vii) $f^{-1}(E \setminus F) = f^{-1}(E) \setminus f^{-1}(F)$.

Pf.: (ii) Let $y \in f(f^{-1}(E))$ be arbitrary. Then, $\exists x \in f^{-1}(E)$ s.t. $f(x) = y$. Since $x \in f^{-1}(E)$, then $\exists z \in E$ s.t. $z = f(x)$. But f is a f'n, so $z = f(x) = y$ implies $y = z$, hence $y \in E$. ✓

(iv) Inclusion "$\supset$" is obvious, as $A \subset A \cup B$ and $B \subset A \cup B$. Let then $y \in f(A \cup B)$ be arbitrary. Then, $\exists x \in X$ s.t. $x \in A \cup B \wedge y = f(x)$, or $\exists x \in X$ s.t. $(x \in A \vee x \in B) \wedge y = f(x)$, or $\exists x \in X$ s.t. $(x \in A \wedge y = f(x)) \vee (x \in B \wedge y = f(x))$. Thus, $y \in f(A) \vee y \in f(B)$, or $y \in f(A) \cup f(B)$.

Other claims – exercise. ⊠

Thm. Let $f: X \to Y$ be a function, $A, B \subset X$, $E \subset Y$. Then,

(i) If f is injective, then $f^{-1}(f(A)) = A$

(ii) If f is surjective, then $f(f^{-1}(E)) = E$.

(iii) If f is injective, then $f(A \cap B) = f(A) \cap f(B)$

Pf. (i) Suppose f is injective. It suffices to show that $f^{-1}(f(A)) \subset A$. Let $x \in f^{-1}(f(A))$ be arbitrary. Then, $\exists y \in f(A)$ s.t. $y = f(x)$. Since $y \in f(A)$, then $\exists z \in A$ s.t. $y = f(z)$. Now, $f(x) = y = f(z)$, so by injectivity, $x = z \in A$. ✓

(ii) Suppose f is surjective. Let $y \in E$ be arbitrary. By surjectivity, $\exists x \in X$ s.t. $y = f(x)$. Then, $x \in f^{-1}(E)$, and so $y = f(x) \in f(f^{-1}(E))$. ✓

(iii) Suppose f is injective. Let $y \in f(A) \cap f(B)$ be arbitrary. We have $y \in f(A) \wedge y \in f(B)$, so $\exists x_1 \in A$ s.t. $y = f(x_1)$ $\wedge$ $\exists x_2 \in B$ s.t. $y = f(x_2)$. Then, $f(x_1) = y = f(x_2)$, hence $x_1 = x_2$, by injectivity. Since $x_1 = x_2 \in B$, then $x_1 \in A \cap B$, and so $y = f(x_1) \in f(A \cap B)$. ∎

Def. (Composite Function)
Given $f: X \to Y$ and $g: Y \to Z$, we define $g \circ f: X \to Z$ as

$$g \circ f = \{(x,z) \in X \times Z : \exists y \in Y \text{ s.t. } (x,y) \in f \wedge (y,z) \in g\}.$$

(Hence, $\forall x \in X$, $(g \circ f)(x) = g(f(x))$.)

Remarks: 1) In general, $g \circ f \neq f \circ g$. E.g., $f(x) = x^2+1$, $g(y) = \sqrt{y}$ $\Rightarrow$ $g \circ f(x) = \sqrt{x^2+1}$, $f \circ g(y) = y+1$.

2) Composition is associative: $f_3 \circ (f_2 \circ f_1) = (f_3 \circ f_2) \circ f_1$

Thm. Let $f: X \to Y$, $g: Y \to Z$ be functions. Then,
(i) If f and g are surjective, then so is $g \circ f$.
(ii) If f and g are injective, then so is $g \circ f$.
(iii) If f and g are bijective, then so is $g \circ f$.
(iv) If $g \circ f$ is surjective, then so is g.
(v) If $g \circ f$ is injective, then so is f.
(vi) If $g \circ f$ is bijective, then g is surjective and f is injective.

Pf. (i)–(iii): Exercise.

(iv) Suppose g is not surjective. Then, $\exists z \in Z$ s.t. $z \notin g(Y)$. Since $f(X) \subseteq Y$, it follows that $(g \circ f)(X) = g(f(X)) \subseteq g(Y)$, and so $z \notin (g \circ f)(X)$. Thus, $g \circ f$ is not surjective. ✓

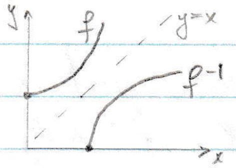
(v) Suppose f is not injective. Then, $\exists x_1 \neq x_2 \in X$ st. $f(x_1) = f(x_2)$. Consequently, $(g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2)$, which proves that $g \circ f$ is not injective. ∎

Def. (Inverse Function) Let $f: X \to Y$ be a bijection. We define the inverse function of f, denoted f^{-1}, as

$$f^{-1} := \{(y,x) \in Y \times X : (x,y) \in f\}.$$

Obs. $\forall x \in X$, $(f^{-1} \circ f)(x) = x$; $\forall y \in Y$, $(f \circ f^{-1})(y) = y$.
Hence, $f^{-1} \circ f = id_X$ and $f \circ f^{-1} = id_Y$ are the identity functions.

Example. $f(x) = x^2+1$ is not bijective as a f'n of $x \in \mathbb{R}$, but $f|_{[0,\infty)} : [0,\infty) \to [1,\infty)$ already is bijective. Set $X = [0,\infty)$, $Y = [1,\infty)$, so $f: X \to Y$ is a bijection. The inverse f'n $f^{-1}: Y \to X$ is given by $f^{-1}(y) = \sqrt{y-1}$ for all $y \in Y = [1,\infty)$.



As subsets of $\mathbb{R}^2$, f and f^{-1} are symmetric about the line $y = x$, b/c $(a,b) \in f \Leftrightarrow (b,a) \in f^{-1}$.

Thm. For any function $f: X \to Y$, one has
$$f = f \circ id_X \quad \text{and} \quad f = id_Y \circ f.$$

Pf. Let $x \in X$ be arbitrary. We have $(f \circ id_X)(x) = f(id_X(x)) = f(x)$. ✓
Similarly, $(id_Y \circ f)(x) = id_Y(f(x)) = f(x)$. ∎

Thm. Let $f: X \to Y$, $g: Y \to Z$ be bijections. Then, $g \circ f$ is a bijection, and its inverse satisfies: $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Pf. We already proved that $g \circ f$ is bijective, and so it has an inverse. Now, by above theorem and the observation,
$$f^{-1} \circ g^{-1} = (f^{-1} \circ g^{-1}) \circ id_Z = f^{-1} \circ g^{-1} \circ (g \circ f) \circ (g \circ f)^{-1} = f^{-1} \circ \overbrace{(g^{-1} \circ g)}^{id_Y} \circ f \circ (g \circ f)^{-1} =$$
$$= f^{-1} \circ (id_Y \circ f) \circ (g \circ f)^{-1} = f^{-1} \circ f \circ (g \circ f)^{-1} = id_X \circ (g \circ f)^{-1} = (g \circ f)^{-1}. \blacksquare$$

Thm. Let $f: X \to Y$ be any function, and suppose $g: Y \to X$ is a function such that $g \circ f = id_X$ and $f \circ g = id_Y$. Then, f is bijective and $g = f^{-1}$.

Pf. Since id_X is injective and $id_X = g \circ f$, then f is injective.
Since id_Y is surjective and $id_Y = f \circ g$, then f is surjective.
Thus, f is bijective and f^{-1} exists. Now,
$$f^{-1} = f^{-1} \circ id_Y = f^{-1} \circ (f \circ g) = (f^{-1} \circ f) \circ g = id_X \circ g = g. \blacksquare$$