Foundations of Mathematics
MATH 220
FALL 2017 Lecture Notes

These notes form a brief summary of what has been covered during the lectures.

All the definitions must be memorized and understood. Statements of important theorems labelled in the margin with the symbol ♣ must be memorized and understood.

Proofs that you are expected to be able to reproduce and that are fundamental are labelled with the symbol ♦ in the margin.

Contents

CHAPTER 1

Introduction to Mathematical Logic

1. Mathematical Language

1.1. Propositions and predicates.

DEFINITION 1. A *proposition* is any declarative sentence that is either true or false.

Characteristics of propositions:

- a proposition has a truth value;
- a proposition is either true or false;
- a proposition cannot be neither true nor false;
- a proposition cannot be true and false.

We will often represent propositions with capital letters, such as P, Q, ... Mathematical propositions are commonly written with symbols for convenience but should be thought of as full-fledged sentences.

EXAMPLE 1. $3 + 5 = 8$.

EXAMPLE 2. $3 + 5 = 9$

DEFINITION 2. A *predicate* is any declarative sentence containing one or more variables that is not a proposition but becomes a proposition when the variables are assigned values.

EXAMPLE 3. $x + 1 = 2$.

EXAMPLE 4. $n + m$ is odd.

A predicate is usually written $P(n)$, $Q(x, y)$, and variants thereof, depending on the number of variables and the letters used for the variables and the statements.

2. Logical connectives

We have two types of mathematical statements: propositions and predicates. We can build more complicated statements using logical connectives. In the sequel P,Q, R are statements letters and represent propositions or predicates.

DEFINITION 3. Let P and Q be statements.

(1) The conjunction of P and Q is the statement "P and Q". The notation for the conjunction of P and Q is $P \wedge Q$ and reads "P and Q".
(2) The disjunction of P and Q is the statement "P or Q". The notation for the disjunction of P and Q is $P \vee Q$ and reads "P or Q".

EXAMPLE 5. The predicate $|x| > 3$ is the disjunction of two predicates $P(x)$, $Q(x)$ where $P(x) : x > 3$, $Q(x) : x < -3$.

DEFINITION 4. If P is a statement, the negation of P is the statement "not P".

We use the notation $\neg P$, which reads "not P" for the negation of P. If P is a proposition only the following two cases can occur: either (P is true and $\neg P$ is false) or (P is false and $\neg P$ is true).

TERMINOLOGY. Expressions of the form $P \wedge Q$, $P \vee Q$, $\neg P$, and so on, where P and Q are variables representing statements are called statement forms. They are not actually propositions or predicates themselves but become propositions (resp. predicates) when the variables P and Q are replaced by propositions (resp. predicates).

Truth tables for statement forms are tables that give the truth value of the statement form in terms of the truth values of the variables.

EXAMPLE 6 (Truth table of conjunction, disjunction, negation).

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

TABLE 1. Conjunction

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

TABLE 2. Disjunction

P	$\neg P$
T	F
F	T

TABLE 3. Negation

DEFINITION 5. We say that two statement forms are logically equivalent if they have the same truth tables.

THEOREM 1 (DeMorgan's Laws).

(1) $\neg(P \wedge Q)$ *is logically equivalent to* $(\neg P) \vee (\neg Q)$.
(2) $\neg(P \vee Q)$ *is logically equivalent to* $(\neg P) \wedge (\neg Q)$.

PROOF.

□

DEFINITION 6. A statement form that is always true no matter what are the truth values of the variables is called a *tautology*.

DEFINITION 7. A statement form that is always false no matter what are the truth values of the variables is called a *contradiction*.

Note that if S is a tautology then $\neg S$ is a contradiction and vice-versa.

EXAMPLE 7. $P \vee (\neg P)$ is a tautology.

EXAMPLE 8. $P \wedge (\neg P)$ is a contradiction.

EXAMPLE 9. Assume that x is a fixed real number. What is the negation of $0 < x < 1$. Find a useful denial of the statement $0 < x < 1$?

SOLUTION.

□

2.1. Implication, contrapositive, converse, biconditional. Roughly speaking an implication is a statement with an "if-then" structure. The "if" part of the statement gives the premise or assumption that is made, and P is called the hypothesis or antecedent. The "then" part is the conclusion that is asserted from the premise and Q is called the conclusion or consequent.

DEFINITION 8. Let P and Q be statements. The implication "$P \implies Q$" (read "P implies Q") is the statement "If P, then Q."

There is no sense of causality in the statement "$P \implies Q$" and P might be (apparently) entirely unrelated to Q. The *only* case when an implication is false is when P is true and Q is false. In particular a false proposition implies anything!

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

TABLE 4. Truth table of the implication

THEOREM 2. *(1) The statement form $P \implies Q$ and the statement form $(\neg P) \vee Q$ are logically equivalent.*
(2) The statement form $\neg(P \implies Q)$ and the statement form $P \wedge \neg Q$ are logically equivalent.

PROOF.

□

DEFINITION 9. Let P and Q be statements. The statement $\neg Q \implies \neg P$ is called the contrapositive of the statement $P \implies Q$.

THEOREM 3.
The statement form $P \implies Q$ and the statement form $(\neg Q) \implies (\neg P)$ are logically equivalent.

PROOF.

P	Q	$\neg Q \implies \neg P$
T	T	T
T	F	F
F	T	T
F	F	T

□

DEFINITION 10. Let P, Q be statements. The statement $Q \implies P$ is called the converse of the statement $P \implies Q$.

THEOREM 4. *The statement form $P \implies Q$ and the statement form $Q \implies P$ are NOT logically equivalent.*

PROOF.

P	Q	$Q \implies P$
T	T	T
T	F	T
F	T	F
F	F	T

□

DEFINITION 11. Let P and Q be statements. The statement $Q \iff P$ (or P iff Q, read P if and only if Q) is the statement $(P \implies Q) \wedge (Q \implies P)$. The symbol $\iff$ is called the biconditional.

Consider the implication "$P \implies Q$". We say that P is a *sufficient condition* for Q, because in order for Q to be true it is sufficient that P be true. Also, we say that Q is a *necessary condition* for P meaning that Q must be true in order for P to be true, or in other words if Q is false then P is false.

3. Quantifiers

Another way a predicate can be made into a proposition is by modifying it with a quantifier that acts on the free variable which lives in a certain ambient universe. If $P(x)$ is a predicate, then the proposition "$(\forall x)P(x)$" (read "for all x, $P(x)$") is a mathematical statement with a truth value. The symbol $\forall$ is called the *universal*

quantifier. The statement $(\forall x)P(x)$ is true exactly when each individual element a in the ambient universe has the property that $P(a)$ is true.

If $P(x)$ is a predicate, then the proposition "$(\exists x)P(x)$" (read "there exists x such that $P(x)$") is also a mathematical statement with a truth value. The symbol $\exists$ is called the *existential quantifier*. The statement $(\exists x)P(x)$ is true exactly when at least one individual element a in the ambient universe has the property that $P(a)$ is true.

TERMINOLOGY. A variable x is called a bound variable once a quantifier is applied to x. Otherwise we say that x is a free variable.

EXAMPLE 10. Discuss the truth values of the following statements.

(1) $(\forall x)x + 5 = 8$.
(2) $(\exists x)x + 5 = 8$.
(3) $(\exists n)n + 5 = \pi$.

REMARK 1. Since the truth values of statements depend on the intended universe we will usually make it explicit unless it is clear from the context. An important notion in mathematical logic is the notion of "membership". To say that a free variable belongs to the intended universe $\mathcal{U}$, we write $x \in \mathcal{U}$. We can modify a quantifier by restricting the free variable to live in the intended universe $\mathcal{U}$, and we write $(\forall x \in \mathcal{U})$ (read "for all x in $\mathcal{U}$") or $(\exists x \in \mathcal{U})$ (read "there exists x in $\mathcal{U}$"). The notation

$$(\forall x \in \mathcal{U})P(x)$$

will be used as an abbreviation for

$$(\forall x)[x \in \mathcal{U} \implies P(x)].$$

Similarly, the notation

$$(\exists x \in \mathcal{U})P(x)$$

will be used as an abbreviation for

$$(\exists x)[x \in \mathcal{U} \wedge P(x)].$$

The two basic rules to negate statements with quantifiers:

Rule 1: The negation of the statement "$(\forall x)P(x)$" is the statement "$(\exists x)\neg P(x)$".
Rule 2: The negation of the statement "$(\exists x)P(x)$" is the statement "$(\forall x)\neg P(x)$".

Numerous other rules can be derived from Rule 1 and Rule 2.

EXAMPLE 11. The negation of "$(\forall x)(\exists y)P(x, y)$" is "$(\exists x)\neg[(\exists y)P(x, y)]$" which is "$(\exists x)(\forall y)\neg P(x, y)$".

EXAMPLE 12. Let $\mathcal{U}$ be the intended universe.

(1) Find a useful denial of the proposition "$(\forall x \in \mathcal{U})P(x)$"?
(2) Find a useful denial of the proposition "$(\exists x \in \mathcal{U})P(x)$"?

SOLUTION.

□

Most often we will be interested in establishing the truth of statements of the form "$\forall x, P(x) \implies Q(x)$". We might deal with more that one common variable.

Remark 2. In practice it is usually simpler and more convenient to use the same letter for the variable and its assigned value. We will do it from now on.

CHAPTER 2

Classical Proof Techniques

1. Modus Ponens

Recall that the truth table of the implication is:

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

Modus ponens is a logical arguments that exploits the first row in the table and says that "Q is true" is a valid conclusion based in the hypotheses that "P is true" and "$P \implies Q$ is true".

Example 13. You know from your Calculus course that $P(f) \implies Q(f)$ is true where,

$$P(f) : \text{The function } f \text{ is differentiable at } 0,$$
$$Q(f) : \text{The function } f \text{ is continuous at } 0.$$

Therefore you can conclude that $Q(f)$ is true if you know that $P(f)$ is true.

2. Direct proofs

2.1. Statement of the form $(\forall x)P(x)$.

Proof Technique 1 (Universal statements). *To prove a statement of the form $(\forall x)P(x)$ is true directly we proceed as follows:*

- *We begin with "Let x be a fixed but arbitrary element of the intended universe."*
- *We must then demonstrate that $P(x)$ is true.*

Example 14. Prove that for all $n \in \mathbb{N}$, $6n + 5$ is odd.

Solution.

□

2.2. Statement of the form $(\exists x)P(x)$.

PROOF TECHNIQUE 2 (Existential statements). *To prove a statement of the form $(\exists x)P(x)$ is true directly we proceed as follows:*

- *We must find an element a in the intended universe and demonstrate that $P(a)$ is true.*

EXAMPLE 15. Show that there exists $x \in \mathbb{R}$ such that $x^2 + x - 1 = 0$.

SOLUTION.

□

2.3. Statement of the form $(\forall x)[P(x) \implies Q(x)]$.

PROOF TECHNIQUE 3 (Implications). *According to the truth table of the implication, to prove a statement of the form $(\forall x)[P(x) \implies Q(x)]$ is true directly we proceed as follows:*

- *We begin with "Assume that $P(x)$ is true."*
- *We must then demonstrate that $Q(x)$ is true.*

EXAMPLE 16. Prove that if n is even, then n^2 is even.

SOLUTION.

□

2.4. Proof by cases.

EXAMPLE 17. Prove that for all real numbers x and y, $|x + y| \leq |x| + |y|$.

SOLUTION.

□

2.5. Working backwards.

EXAMPLE 18. Prove that for all positive real numbers x, $\frac{x}{x+1} < \frac{x+1}{x+2}$.

SOLUTION.

□

2.6. Proving biconditional statements.

EXAMPLE 19. Prove that for all numbers $x, y \in \mathbb{R}$ with $y \geq 0$, $|x| \leq y$ if and only if $-y \leq x \leq y$.

SOLUTION.

□

2.7. Uniqueness proofs. Let $P(x)$ be a predicate. There are two equivalent ways to express the statement "there exists a unique x such that $P(x)$":

$$(\exists x)[P(x) \wedge (\forall y)[P(y) \implies (x = y)]]$$

or

$$[(\exists x)P(x)] \wedge [(\forall y)(\forall z)[(P(y) \wedge P(z)) \implies (y = z)]].$$

Both statements are abbreviated as $(\exists! x)P(x)$.

PROOF TECHNIQUE 4 (Uniqueness). *To prove that there exists a unique x such that $P(x)$ is true we can proceed in two different ways.*
Either,

- *we find an element a in the intended universe and demonstrate that $P(a)$ is true,*
- *and then we demonstrate that if there exists b such that $P(b)$ is true then $a = b$.*

Or,

- *we prove first that if there exist x, y such that if $P(x) \wedge P(y)$ is true then $x = y$,*
- *and then we find an element a in the intended universe and demonstrate that $P(a)$ is true,*

EXAMPLE 20. Prove that if an integer has an additive inverse then this inverse is unique.

SOLUTION.

□

2.8. Counterexamples. Let P and Q be statements. Recall that,

P	Q	$\neg(P \implies Q)$	$P \wedge \neg(Q)$
T	T	F	F
T	F	T	T
F	T	F	F
F	F	F	F

and hence $\neg(P \implies Q)$ is logically equivalent to $P \wedge \neg(Q)$. Since the negation of the statement $(\forall x)[P(x) \implies Q(x)]$ is the statement $(\exists x)\neg[P(x) \implies Q(x)]$, the negation of $(\forall x)[P(x) \implies Q(x)]$ is logically equivalent to $(\exists x)P(x) \wedge \neg Q(x)$. Note that the negation of an implication is *not* an implication!

TERMINOLOGY. An assignment of the variable x (still denoted by x) such that $P(x) \wedge \neg Q(x)$ is true, is called a counterexample for the statement $(\forall x)[P(x) \implies Q(x)]$.

EXAMPLE 21. Is the following statement true or false?
For all positive integers n, $n^2 + n + 41$ is prime.

SOLUTION.

□

3. Indirect Proofs

3.1. Proof by contradiction. A proof by contradiction is based on the observation that the statement form $\neg P \implies [Q \wedge \neg Q]$ is logically equivalent to P.

P	Q	$Q \wedge \neg Q$	$\neg P$	$\neg P \implies [Q \wedge \neg Q]$
T	T	F	F	T
T	F	F	F	T
F	T	F	T	F
F	F	F	T	F

Therefore, in order to prove a statement P, for example, we could assume that P is false and deduce a statement that we know is false (like $0 = 1$ or $\frac{1}{2}$ is an integer...).

PROOF TECHNIQUE 5 (Proof by contradiction). *To prove a statement P is true by contradiction we proceed as follows:*

- *We begin with "Assume $\neg P$ is true."*
- *We deduce a contradiction.*
- *We then conclude that P is true.*

EXAMPLE 22. Prove that there does not exist integers m and n such that $15m + 5n = 81$.

SOLUTION:

□

3.2. Proving the contrapositive. The statement forms $P \implies Q$ and $\neg Q \implies \neg P$ are logically equivalent.

PROOF TECHNIQUE 6 (Proof by contrapositive). *To prove $P \implies Q$ one may choose instead to prove $\neg Q \implies \neg P$.*

EXAMPLE 23. Is the following statement true?

$$(\forall n)[(\exists k)(k \in \mathbb{N}) \wedge (n^2 = 2k + 1))] \implies [(\exists k)(k \in \mathbb{N}) \wedge (n = 2k + 1)]$$

SOLUTION:

□

3.3. Proving disjunction statements. Let P and Q be statements. To prove disjunction statements we can use the observation that $P \vee Q$, $\neg P \implies Q$, and $\neg Q \implies P$ are logically equivalent.

P	Q	$P \vee Q$	$\neg P \implies Q$	$\neg Q \implies P$
T	T	T	T	T
T	F	T	T	T
F	T	T	T	T
F	F	F	F	F

PROOF TECHNIQUE 7 (Proving disjunction statements). *To prove a statement $P \vee Q$ is true, we may either assume that $\neg P$ and prove Q, or assume $\neg Q$ and prove P.*

EXAMPLE 24. Prove that for all real numbers x and y with $y \geq 0$, if $x^2 \geq y$, then $x \geq \sqrt{y}$ or $x \leq -\sqrt{y}$

SOLUTION:

□

4. Existence of Irrational Numbers

In this section we will prove the following theorem.

THEOREM 5. *The real number $\sqrt{2}$ is irrational.* ♦♣

Recall that a number x is irrational if it is not rational, *i.e.,*

$$\neg \left[(\exists p \in \mathbb{N})(\exists q \in \mathbb{Z}^+)\big[\frac{p}{q} = x\big] \right]$$

HINT. Prove Theorem 5 by contradiction. □

PROOF OF THEOREM 5.

□

5. Euclid Theorem

In this section we will prove the following theorem.

♦♣

THEOREM 6 (Euclid). *There are infinitely many prime numbers.*

A natural number p is prime if

$$p > 1 \text{ and } (\forall m, n \in \mathbb{N})[p = mn \implies (m = 1 \vee n = 1)].$$

We will assume the Fundamental Theorem of Arithmetic, which states that every positive integer greater than 1 can be written as a product of primes. Furthermore, this product of primes is unique, except for the order in which the factors appear.

HINT. Prove Theorem 6 by contradiction. □

PROOF OF THEOREM 6.

□

6. Statements with mixed quantifiers

When a statement involves several quantifiers the order usually matters!

EXAMPLE 25. Let $P(x, y)$ be a predicate with two variables. Is the proposition

$$(\forall x)(\exists y)P(x, y)$$

logically equivalent to the proposition

$$(\exists y)(\forall x)P(x, y)?$$

SOLUTION. No. One cannot swap quantifiers without care!

"For all odd number n there exists a number $k \in \{0, 1, 2, \dots, \}$ such that $n = 2k + 1$" is a true statement, while "there exists a number $k \in \{0, 1, 2, \dots, \}$ such that for all odd number n, $n = 2k + 1$" is clearly a false statement. □

The definition of the limit of a function at a point involves three quantifiers.

DEFINITION 12. Let $x_0 \in (a, b)$, $\ell \in \mathbb{R}$ and $f\colon (a, x_0) \cup (x_0, b) \to \mathbb{R}$. We say that ℓ is the limit of f at x_0, and we write $\lim_{x\to x_0} f(x) = \ell$, if for all $\varepsilon > 0$ there exists $\delta > 0$ such that if x satisfies $0 < |x - x_0| < \delta$ then $|f(x) - \ell| < \varepsilon$. Symbolically, $\lim_{x\to x_0} f(x) = \ell$ if

$$(\forall \varepsilon > 0)(\exists \delta > 0)(\forall x)[0 < |x - x_0| < \delta \implies |f(x) - \ell| < \varepsilon].$$

EXERCISE 1. Let $f(x) = \begin{cases} 4x - 1 \text{ if } x \neq 1 \\ 2 \text{ if } x = 1. \end{cases}$

Prove that $\lim\limits_{x\to 1} f(x) = 3$

SOLUTION.

□

CHAPTER 3

Induction

1. Principle of Mathematical Induction

The principle of mathematical induction is a very powerful tool to deal with infinite objects and to prove rigorously infinitely many (in the sense that they can be enumerated) statements.

THEOREM 7 (Principle of Mathematical Induction). *For every natural number n, let $P(n)$ be a predicate. Suppose that there exists $k_0 \in \mathbb{N}$ such that*

Base case: *$P(k_0)$ is true.*
and
Induction Step: *for all $k \geq k_0$, $P(k+1)$ is true under the assumption that $P(k)$ is true,*
Conclusion: *then for all $k \geq k_0$ $P(k)$ is true.*

The principle of mathematical induction is most commonly used with $k_0 = 0$ or $k_0 = 1$.

EXAMPLE 26. Show that for all $n \geq 1$, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

SOLUTION: For all $n \in \mathbb{N}$, let $P(n)$ be the predicate $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Base case: Since $\sum_{i=1}^{1} i = 1$ and $\frac{1(1+1)}{2} = 1$, one has that $\sum_{i=1}^{1} i = \frac{1(1+1)}{2}$ and $P(1)$ is true.
Induction Step: Let $k \geq 1$ and assume that $P(k)$ is true, i.e. we assume that $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$. Then,

$$\begin{aligned}\sum_{i=1}^{k+1} i &= \sum_{i=1}^{k} i + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) \text{ (by the induction hypothesis)} \\ &= \frac{(k+1)(k+2)}{2},\end{aligned}$$

and hence $P(k+1)$ is true.

Conclusion By the Principle of Mathematical Induction, one can conclude that $\forall n \geq 1$, $P(n)$ is true, which means that for all $n \geq 1$, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. □

2. Principle of Strong Mathematical Induction

THEOREM 8 (Principle of Strong Mathematical Induction). *For every natural number n, let $P(n)$ be a predicate. Suppose that there exists $k_0 \in \mathbb{N}$ such that*

Base case: *$P(k_0)$ is true,*
and
Induction step: *for all $k \geq k_0$, $P(k+1)$ is true under the assumption that for all $r \in \{k_0, k_0+1, \ldots, k\}$ $P(r)$ is true,*
Conclusion: *then for all $n \geq k_0$ $P(n)$ is true.*

EXERCISE 2. Consider the sequence $(a_n)_{n=1}^{\infty}$ recursively defined as $a_1 = 1$, $a_2 = 5$ and for all $n \geq 2$, $a_{n+1} = a_n + 2a_{n-1}$. Show that for all $n \geq 1$, $a_n = 2^n + (-1)^n$.

SOLUTION: For all $n \in \mathbb{N}$, let $P(n)$ be the predicate $a_n = 2^n + (-1)^n$.

Base case: Since $a_1 = 1$ and $2^1 + (-1)^1 = 2 - 1 = 1$, one has that $a_1 = 2^1 + (-1)^1$ and $P(1)$ is true.

Induction Step: Let $k \geq 1$ and assume that for all $r \in \{1, 2, \ldots, k\}$ $P(r)$ is true, i.e. we assume that for all $r \in \{1, 2, \ldots, k\}$ $a_r = 2^r + (-1)^r$. We want to show that $P(k+1)$ is true. In this problem, the case $k = 2$ has to be treated separately. If $k = 2$, observe that $P(2)$ is true (regardless of the truth value of $P(1)$) since $2^2 + (-1)^2 = 5 = a_2$ and thus in particular if $P(1)$ is true then $P(2)$ is true. Otherwise, if $k \geq 2$, assuming $P(1), P(2), \ldots, P(k)$ are true, then

$$\begin{aligned} a_{k+1} &= a_k + 2a_{k-1} \text{ (here we need } k \geq 2 \text{ since } a_0 \text{ is not defined)} \\ &= 2^k + (-1)^k + 2(2^{k-1} + (-1)^{k-1}) \text{ (by the induction hypothesis)} \\ &= 2 \cdot 2^k + (-1)^{k-1}(-1 + 2) \\ &= 2^{k+1} + (-1)^{k+1} \text{ (since } (-1)^{k+1} = (-1)^{k-1}), \end{aligned}$$

and hence $P(k+1)$ is true.

Conclusion: By the Principle of Strong Mathematical Induction, one can conclude that for all $n \geq 1$, $P(n)$ is true, which means that for all $n \geq 1$, $a_n = 2^n + (-1)^n$.

□

THEOREM 9 (Fundamental Theorem of Arithmetic). *Every positive integer greater than* 1 *can be written as a product of primes. Furthermore, this product of primes is unique, except for the order in which the factors appear.*

PROOF.

□

3. Exercices

EXERCISE 3. Show that the following equalities hold.

(1) for all $n \geq 1$, $\sum_{i=1}^{n}(2i-1) = n^2$.
(2) for all $n \geq 1$, $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.
(3) for all $n \geq 1$, $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$.
(4) for all $n \geq 1$, $\sum_{i=1}^{n}(2i-1)^2 = \frac{(2n-1)(2n)(2n+1)}{6}$.
(5) for all $n \geq 1$, $\sum_{i=1}^{n}(2i)^2 = \frac{2n(2n+1)(2n+2)}{6}$.

EXERCISE 4. Prove that for all $n \geq 5$, $2^n > n^2$.

EXERCISE 5. Prove that for all $n \geq 4$, $2^n \leq n!$.

EXERCISE 6. If r is any real number different from 1, prove that for all $n \geq 0$,

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}.$$

EXERCISE 7. Assuming that $(1+\frac{1}{n})^n < e$, for all $n \geq 1$, prove that for all $n \geq 1$, $n! > (\frac{n}{e})^n$.

EXERCISE 8. Let n be an integer. Show that if n is even then n^k is even for all $k \in \mathbb{N}$.

EXERCISE 9. Consider the sequence $(a_n)_{n=1}^{\infty}$ recursively defined as $a_1 = 1$, $a_2 = 8$ and for all $n \geq 3$, $a_n = a_{n-1} + 2a_{n-2}$. Show that for all $n \geq 1$, $a_n = 3 \cdot 2^{n-1} + 2(-1)^n$.

EXERCISE 10. Consider the sequence $(a_n)_{n=1}^{\infty}$ recursively defined as $a_1 = 2$, $a_2 = 4$ and for all $n \geq 3$, $a_n = 3a_{n-1} - 2a_{n-2}$. For all $n \geq 1$, find a closed formula for a_n.

CHAPTER 4

Introduction to Elementary Set Theory

1. Sets and subsets

We won't give a formal definition of the notion of a set but we will understand the word set as an undefined term which refers to a collection of objects. The objects in a set are called elements and we use the notation $x \in X$ to express that the element x is in the set X. The notion of membership is also not formally defined and is part of the concept of a set. We use the abbreviation $x \notin X$ for $\neg(x \in X)$.

Axiom: There is a set with no elements which is called the empty set and is denoted by $\emptyset$.

Observe that $x \in \emptyset$ is always false regardless of the element x that is under consideration, and thus $x \notin \emptyset$ is always true.

EXAMPLE 27. Classical sets.

(1) $\mathbb{R}$ real numbers
(2) $\mathbb{Q} := \{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0\}$ rational numbers
(3) $\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$ integers
(4) $\mathbb{N} := \{1, 2, 3, \dots\}$ natural numbers

DEFINITION 13 (Truth set for a predicate). Let $P(x)$ be a predicate and U be the ambient set. The set $A := \{x \in U |\ P(x) \text{ is true}\}$ is called the truth set of the predicate $P(x)$.

EXAMPLE 28. (1) $\{x \in \mathbb{Z} \mid (\exists k \in \mathbb{Z})[x = 5k]\}$
(2) $\{x \in \mathbb{R} \mid (x > 0) \wedge (x^2 \in \mathbb{Z}^+)\}$

DEFINITION 14 (Subset). Let X and Y be sets. We say that X is a subset of Y, and write $X \subseteq Y$, if every element of X is also an element of Y. Formally, $X \subseteq Y$ if $(\forall x)[x \in X \implies x \in Y]$.

REMARK 3. The expression $X \subseteq Y$ is a very convenient abbreviation for the proposition $(\forall x)[x \in X \implies x \in Y]$. To prove that $X \subseteq Y$ you need to prove an *implication* with a *universal* quantifier.

EXAMPLE 29. $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$

EXERCISE 11. We write $x \nsubseteq X$ for $\neg(x \subseteq X)$. Give a formal statement expressing $x \nsubseteq X$.

SOLUTION:

□

EXERCISE 12. Prove that $X \subseteq Y$ where $X = \{n \in \mathbb{Z} \mid n \text{ is a multiple of } 4\}$ and $Y = \{n \in \mathbb{Z} \mid n \text{ is even}\}$

SOLUTION:

□

EXERCISE 13. Prove that $X = \{n \in \mathbb{Z} \mid n + 5 \text{ is odd}\}$ is the set of all even integers.

SOLUTION:

□

PROPOSITION 1 (Transitivity of the subset relation). *Let X, Y, and Z be sets, and suppose that $X \subseteq Y$ and $Y \subseteq Z$. Then $X \subseteq Z$.*

PROOF. (Hint: Direct proof.)

□

DEFINITION 15 (Equality). We say that two sets X and Y are equal, written $X = Y$, if they have the same elements.
Equivalently, using the notion of inclusion $X = Y$ if $X \subseteq Y$ and $Y \subseteq X$. Formally, $X = Y$ if $(\forall x)[x \in X \iff x \in Y]$.

If X is a subset of Y and $X \neq Y$, we write $X \subset Y$ and say that X is a proper subset of Y.

2. Operation on sets

2.1. Union and intersection of two sets.

DEFINITION 16 (Union). Let X and Y be sets. The union of X and Y, denoted $X \cup Y$, is the set of all elements that belong to X or to Y. Formally,

$$X \cup Y = \{z \mid (z \in X) \vee (z \in Y)\}.$$

DEFINITION 17 (Intersection). Let X and Y be sets. The intersection of X and Y, denoted $X \cap Y$, is the set is the set of all elements that belong to X and to Y. Formally,

$$X \cap Y = \{z \mid (z \in X) \wedge (z \in Y)\}.$$

We say that two sets are *disjoint* if their intersection is the empty set.

PROPOSITION 2 (Commutativity Properties). *Let X and Y be sets. Then,*

(1) $X \cup Y = Y \cup X$
(2) $X \cap Y = Y \cap X$

PROOF. (1) (Hint: You could use that $P \vee Q$ is logically equivalent to $Q \vee P$ or write a double-inclusion proof)

(2) (Hint: You could use that $P \wedge Q$ is logically equivalent to $Q \wedge P$ or write a double-inclusion proof)

□

PROPOSITION 3 (Associativity Properties). *Let X, Y, Z be sets. Then,*

(1) $(X \cup Y) \cup Z = X \cup (Y \cup Z)$
(2) $(X \cap Y) \cap Z = X \cap (Y \cap Z)$

PROOF. (1) (Hint: You could use that $(P \vee Q) \vee R$ is logically equivalent to $P \vee (Q \vee r)$ or write a double-inclusion proof)

(2) (Hint: You could use that $(P \wedge Q) \wedge R$ is logically equivalent to $P \wedge (Q \wedge P)$ or write a double-inclusion proof)

□

PROPOSITION 4 (Properties of the empty set). *Let X be a set. Then,*

(1) $\emptyset \subseteq X$
(2) $X \cup \emptyset = X$
(3) $X \cap \emptyset = \emptyset$

PROOF. (1) (Hint: Use the fact that an implication is true if the assumption is false.)

(2) (Hint: You could use the fact that when P is false then $(P \vee Q)$ is logically equivalent to Q or write a double-inclusion proof)

(3) (Hint: You could use that if P is false then $P \wedge Q$ is always false or write a double-inclusion proof)

□

THEOREM 10 (Distributivity Properties). *Let X, Y, Z be sets. Then,*

(1) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$
(2) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$

PROOF. (1) (Hint: You could use that $P \wedge (Q \vee R)$ is logically equivalent to $(P \wedge Q) \vee (P \wedge R)$ or write a double-inclusion proof)

(2) (Hint: You could use that $P \vee (Q \wedge R)$ is logically equivalent to $(P \vee Q) \wedge (P \vee R)$or write a double-inclusion proof)

□

PROPOSITION 5 (Other useful properties). *Let X and Y be sets. Then,*

(1) $X \subseteq X \cup Y$ *and* $Y \subseteq X \cup Y$
(2) $X \cap Y \subseteq X$ *and* $X \cap Y \subseteq Y$
(3) $X \subseteq Y \iff X \cup Y = Y$
(4) $X \subseteq Y \iff X \cap Y = X$

PROOF.

(1)

(2)

(3)

□

2.2. Complement.

DEFINITION 18 (Complement). Let X and Y be sets. The complement of X in Y, denoted $Y - X$, is the set of elements that are in Y but not in X. Formally,

$$Y - X = \{z \mid (z \in Y) \wedge (z \notin X)\}.$$

For convenience, if U is the ambient set, the set $U - X$ will be simply denoted by $\overline{X}$, and called the complement of X and $\overline{X} = \{z \mid z \notin X\}$.

REMARK 4.
(1) The definition of the complement of X in Y does NOT assume that either set be a subset of the other.
(2) Note that if U is the ambient set the $\overline{U} = \emptyset$ and $\overline{\emptyset} = U$.
(3) Equivalently $X - Y = X \cap \overline{Y}$.

THEOREM 11 (DeMorgan's Laws). *Let X and Y be subsets of a universal set U. Then*

♦♣

(1) $\overline{X \cup Y} = \overline{X} \cap \overline{Y}$,
(2) $\overline{X \cap Y} = \overline{X} \cup \overline{Y}$.

We will give two conceptually different proofs: "the mathematician's proof" and "the logician's proof". The mathematician's proof is a basic-double inclusion proof and uses the logic of connectives implicitely. The logician will argue that the equality holds since he, or she, will recognize that the truth of the statement follows from the logical equivalence of two statement forms.

DOUBLE-INCLUSION PROOFS.
(1) Let $z \in \overline{X \cup Y}$ then $z \notin X \cup Y$ (by definition of the complement), and it follows that $z \notin X$ and $z \notin Y$ (by definition of the union). Thus, $z \in \overline{X}$ and $x \in \overline{Y}$ (by definition of the complement), which means that $z \in \overline{X} \cap \overline{Y}$ (by definition of the intersection). We just proved that $\overline{X \cup Y} \subseteq \overline{X} \cap \overline{Y}$.

For the reverse inclusion, let $z \in \overline{X} \cap \overline{Y}$, then $z \in \overline{X}$ and $z \in \overline{Y}$ (by definition of the intersection), and thus $z \notin X$ and $z \notin Y$ (by definition of the complement). It follows that $z \notin X \cup Y$ (by definition of the union), and hence $z \in \overline{X \cup Y}$ (by definition of the complement). This shows the reverse inclusion.

(2) Let $z \in \overline{X \cap Y}$ then $z \notin X \cap Y$ (by definition of the complement), and it follows that $z \notin X$ or $z \notin Y$ (by definition of the intersection). Thus, $z \in \overline{X}$ or $z \in \overline{Y}$ (by definition of the complement), which means that $z \in \overline{X} \cup \overline{Y}$ (by definition of the union). We just proved that $\overline{X \cap Y} \subseteq \overline{X} \cup \overline{Y}$.

For the reverse inclusion, let $z \in \overline{X} \cup \overline{Y}$, then $z \in \overline{X}$ or $z \in \overline{Y}$ (by definition of the union), and thus $z \notin X$ or $x \notin Y$ (by definition of the complement). It follows that $z \notin X \cap Y$ (by definition of the intersection), and hence $z \in \overline{X \cap Y}$ (by definition of the complement). This shows the reverse inclusion.

□

PROOFS THAT REDUCE TO AN ARGUMENT IN PROPOSITIONAL LOGIC. (1) If one considers the predicates $P(z)$: "$z \in X$" and $Q(z)$: "$z \in Y$". From the logic standpoint $\overline{X \cup Y} = \overline{X} \cap \overline{Y}$ is actually a convenient abbreviation for the proposition

$$(\forall z \in U)[\neg(P(z) \vee Q(z)) \iff (\neg P(z) \wedge \neg Q(z))].$$

But, we have proven that $\neg(P \vee Q)$ is logically equivalent to $(\neg P \wedge \neg Q)$ no matter what statements are substituted for P and we can conclude that the equality actually holds!

(2) One more time the equality holds since from the logic standpoint $\overline{X \cap Y} = \overline{X} \cup \overline{Y}$ is actually a convenient abbreviation for the statement

$$(\forall z \in U)[\neg(P(z) \wedge Q(z)) \iff (\neg P(z) \vee \neg Q(z))].$$

But, as we have proven that $\neg(P \wedge Q)$ is logically equivalent to $(\neg P \vee \neg Q)$ we conclude as above.

□

THEOREM 12. *Let X and Y be subsets of some universal set U. Then $X \subseteq Y$ if and only if $\overline{Y} \subseteq \overline{X}$.*

PROOF. (Hint: You can give a proof using formal logic arguments "the logician's proof", or another one using classical mathematical arguments "the mathematician's proof".)

□

2.3. Arbitrary unions and intersections. For all $i \in I$, where I is called the indexing set, let X_i be a subset of some universal set. We use the notation $\{X_i \mid i \in I\}$ or $(X_i)_{i \in I}$ to denote the collection of such sets. In the previous section we defined the union of two sets. Based on the definition of the union of two sets we can naturally recursively define the union of finitely many sets $X_1, X_2, \ldots, X_n$, for $n \geq 2$, this new set will be denoted by $\bigcup_{k=1}^{n} X_k$, as follows:

$$\bigcup_{k=1}^{2} X_k = X_1 \cup X_2,$$

and for $n \geq 3$

$$\bigcup_{k=1}^{n} X_k = (\bigcup_{k=1}^{n-1} X_k) \cup X_n.$$

Since the operation of taking union is associative these new sets are unambiguously defined. Using a similar approach we can define the intersection of finitely many sets. Unfortunately, we cannot use a recursive definition to define arbitrary infinite unions or intersections (e.g. if the index $I = \mathbb{R}$) and we need to proceed differently and define arbitrary unions as the truth set of a certain predicate.

DEFINITION 19 (Arbitrary unions). Let I be a set and $(X_i)_{i\in I}$ be a collection of sets. The union of the collection $(X_i)_{i\in I}$, denoted $\bigcup_{i\in I} X_i$ is the set of all elements that belong to at least one set of the collection. Formally,

$$\{x \mid (\exists i \in I)[x \in X_i]\}.$$

REMARK 5. We can easily show using the principle of mathematical induction that the set $\bigcup_{k=1}^{n} X_k$ that was recursively defined and the set $\bigcup_{i\in\{1,2,\ldots,n\}} X_i$ where $I = \{1, 2, \ldots, n\}$ defined using the truth set coincide and the two definitions are compatible. Since $\bigcup_{k=1}^{n} X_k = \bigcup_{i\in\{1,2,\ldots,n\}} X_i$ we will use both notations interchangeably.

REMARK 6. If $I = \mathbb{N}$ we write $\bigcup_{n=1}^{\infty} X_n$ for $\bigcup_{n\in\mathbb{N}} X_i$.

EXERCISE 14. Let $X_n = [1, 1 + \frac{1}{n}]$ for $n \in \mathbb{N}$. Compute $\bigcup_{i=n}^{\infty} X_n$.

SOLUTION:

□

EXERCISE 15. Let $X_n = (\frac{2}{n}, 2n]$ for $n \geq 2$. Compute $\bigcup_{i=n}^{\infty} X_n$.

SOLUTION:

□

Using a similar approach we can define arbitrary intersections.

DEFINITION 20 (Arbitrary intersections). Let I be a set and $\{X_i \mid i \in I\}$ be a collection of sets. The intersection of the collection, denoted $\bigcap_{i\in I} X_i$ is the set of all elements that belong to all sets of the collection. Formally,

$$\{x \mid (\forall i \in I)[x \in X_i]\}.$$

REMARK 7. If $I = \mathbb{N}$ we write $\bigcap_{n=1}^{\infty} X_i$ for $\bigcap_{n\in\mathbb{N}} X_n$.

EXERCISE 16. Let $X_n = [1, 1 + \frac{1}{n}]$ for $n \in \mathbb{N}$. Compute $\bigcap_{n=1}^{\infty} X_n$.

SOLUTION:

□

EXERCISE 17. Let $X_n = (\frac{2}{n}, 2n]$ for $n \geq 2$. Compute $\bigcap_{n=1}^{\infty} X_n$.

SOLUTION:

□

Most of the theorems from the previous section admit a generalization to arbitrary unions or intersections. Below are some examples.

PROPOSITION 6 (Other useful properties). *Let $(X_i)_{i\in I}$ be a collection of sets. Then,*

(1) $\forall j \in I \ X_j \subseteq \bigcup_{i\in I} X_i$,
(2) $\forall j \in I \ \bigcap_{i\in I} X_i \subseteq X_j$,

PROOF.

(1)

(2)

□

THEOREM 13 (DeMorgan's Laws for arbitrary unions and intersections). *Let* ♦♣ *$(X_i)_{i\in I}$ be a collection of set. Then*

(1) $\overline{\bigcup_{i\in I} X_i} = \bigcap_{i\in I} \overline{X_i}$,

(2) $\overline{\bigcap_{i\in I} X_i} = \bigcup_{i\in I} \overline{X_i}$.

PROOF. (Hint: write a double-inclusion proof or use a purely logical argument)

□

2.4. Cartesian products.

DEFINITION 21 (Cartesian Products). Let X and Y be sets. The Cartesian product of X and Y, written $X \times Y$, is the set of all ordered pairs (x, y) with $x \in X$ and $y \in Y$. Formally,

$$X \times Y = \{(x, y) \mid (x \in X) \wedge (y \in Y)\}.$$

REMARK 8. We are working with *ordered pairs* and $X \times Y$ might *not* be equal to $Y \times X$. Try to provide a simple example.

EXAMPLE 30. The 2-dimensional plane $\mathbb{R}^2$ is the Cartesian product $\mathbb{R} \times \mathbb{R}$.

2.5. Power set. We will now consider sets whose elements are sets themselves.

DEFINITION 22 (Power set). Let X be a set. The power set of X, denoted $P(X)$ or 2^X, is the set of all subsets of X. Formally,

$$P(X) = \{Y \mid Y \subseteq X\}.$$

REMARK 9. Do not forget the empty set in the power set!

REMARK 10. If follows from the definition that $A \subseteq X \iff A \in P(X)$.

EXAMPLE 31. The power set of $X = \{1, 2, 3\}$ is

$$P(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

EXAMPLE 32. The power set of $X = \emptyset$ is

$$P(\emptyset) = \{\emptyset\},$$

and

$$P(P(\emptyset)) = P(\{\emptyset\}) = \big\{\emptyset, \{\emptyset\}\big\},$$

and

$$P(P(P(\emptyset))) = P(P(\{\emptyset\})) = P(\{\emptyset, \{\emptyset\}\}) = \big\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\big\},$$

etc...

THEOREM 14. *Let X and Y be sets. Then,*

$$X \subseteq Y \iff P(X) \subseteq P(Y).$$

PROOF.

□

EXERCISE 18. Show that for all $n \geq 0$, if X is a set with exactly n elements then the number of sets in the power set of X is equal to 2^n.

PROOF. (Hint: By induction.)

□

3. Exercises

EXERCISE 19. Let $X_n = [1, 1 + \frac{1}{n}]$ for $n \in \mathbb{N}$. Compute $\bigcup_{n=1}^{\infty} X_n$ and $\bigcap_{n=1}^{\infty} X_n$.

EXERCISE 20. Let $X_n = (\frac{2}{n}, 2n]$ for $n \geq 2$. Compute $\bigcup_{n=1}^{\infty} X_n$ and $\bigcap_{n=1}^{\infty} X_n$.

DEFINITION 23 (Ascending chain). We say that the sequence of sets $(X_n)_{n=1}^{\infty}$ is increasing, or an ascending chain, if $X_1 \subseteq X_2 \subseteq X_3 \subseteq \cdots \subseteq X_n \subseteq X_{n+1} \subseteq \ldots$. Formally, $(X_n)_{n=1}^{\infty}$ is increasing if

$$(\forall n \in \mathbb{N})[X_n \subseteq X_{n+1}].$$

EXERCISE 21. Show that the sequence of sets $(X_n)_{n=1}^{\infty}$ is increasing if and only if

$$(\forall n \in \mathbb{N})(\forall k \in \mathbb{N})[(n \leq k) \implies (X_n \subseteq X_k)].$$

DEFINITION 24 (Descending chain). We say that the sequence of sets $(X_n)_{n=1}^{\infty}$ is decreasing, or a descending chain, if $X_1 \supseteq X_2 \supseteq X_3 \supseteq \cdots \supseteq X_n \supseteq X_{n+1} \supseteq \ldots$. Formally, $(X_n)_{n=1}^{\infty}$ is increasing if

$$(\forall n \in \mathbb{N})[X_n \subseteq X_{n+1}].$$

EXERCISE 22. Show that the sequence of sets $(X_n)_{n=1}^{\infty}$ is decreasing if and only if for all $n, k \in \mathbb{N}$ if $n \leq k$ then $X_n \supseteq X_k$.

CHAPTER 5

Functions

1. Definition and Basic Properties

A Function between two sets is a correspondence between elements of these two sets that enjoy some special properties.

DEFINITION 25. Let X and Y be nonempty sets. A function from X to Y is a correspondence that assigns to *every* element in X *one and only one* element in Y. Formally, a function from X to Y is a subset $F \subseteq X \times Y$ such that

$$[(\forall x \in X)(\exists! y \in Y)\ (x, y) \in F].$$

REMARK 11. The logical formula

$$[(\forall x \in X)(\exists! y \in Y)\ (x, y) \in F]$$

is equivalent to the logical formula

$$[(\forall x \in X)(\exists y \in Y)\ (x, y) \in F]$$

$$\wedge$$

$$[(\forall x \in X)[((x, y_1) \in F) \wedge ((x, y_2) \in F) \wedge ((x, y_1) = (x, y_2))] \implies (y_1 = y_2)]].$$

Since functions play a central role in set theory and in mathematics in general we use a specific terminology. A function is usually denoted by f (instead of F) and we write $f\colon X \to Y$ to say that f is a function from X to Y (instead of $F \subseteq X \times Y$). Since for every $x \in X$ there is a unique element $y \in Y$ such that $(x, y) \in F$, we prefer a much more convenient functional notation. Therefore, we will denote by $f(x)$ the unique element that is in correspondence with x. If $f(x) = y$ we say that y is the image of x or that x is the preimage of y. We call X the domain of f and Y the codomain.

To show that a correspondence $f\colon X \to Y$ is a function we must check that

$$(\forall x \in X)(\exists y \in Y)[f(x) = y]$$

and

$$(\forall x_1 \in X)(\forall x_2 \in X)[(x_1 = x_2) \implies (f(x_1) = f(x_2))].$$

EXAMPLE 33. Let $X = \{1, 2, 3\}$ and $Y = \{5, 8, 10\}$. The correspondence f defined by $f(1) = f(2) = 10$, $f(3) = 8$ is a function from X to Y.

EXAMPLE 34. The identity function on X is the function $i_X\colon X \to X$ such that for all $x \in X$, $i_X(x) = x$.

EXAMPLE 35. For all $a, b \in \mathbb{R}$ the functions $f_{a,b}\colon \mathbb{R} \to \mathbb{R}$, defined by $f_{a,b}(x) = ax + b$ are called linear functions.

DEFINITION 26 (Equality for functions). Two functions $f_1\colon X_1 \to Y_1$ and $f_2\colon X_2 \to Y_2$ are equal if they have they have the *same* domain, the *same* codomain and their actions on elements in X are the same. Formally, two functions $f_1\colon X_1 \to Y_1$ and $f_2\colon X_2 \to Y_2$ are equal if

$$(X_1 = X_2) \wedge (Y_1 = Y_2) \wedge ((\forall z \in X_1)[f_1(z) = f_2(z)]).$$

DEFINITION 27. Let $f\colon X \to Y$ be a function. The graph of the function f is the set, denoted G_f, of all ordered pairs (x, y) of elements $x \in X$ and $y \in Y$ that are in correspondence. Formally,

$$G_f = \{(x, y) \in X \times Y \mid y = f(x)\}.$$

DEFINITION 28. Let $f\colon X \to Y$ be a function. The image (or the range) of the function f is the set, denoted $\mathrm{Im}(f)$, of all elements in the codomain that are the image of an element in the domain. Formally,

$$\mathrm{Im}(f) = \{y \in Y \mid (\exists x \in X)[y = f(x)]\}.$$

The image of a function is a subset of the codomain of the function.

EXERCISE 23. Let $f(x) = \dfrac{3x+5}{x-2}$. Determine the domain of definition (i.e. the set where the function is well-defined) and the range of f.

SOLUTION:

□

EXERCISE 24. Let $f\colon \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = \begin{cases} n-1 \text{ if } n \text{ is even,} \\ n+3 \text{ if } n \text{ is odd.} \end{cases}$

Determine the image of f.

SOLUTION:

□

2. Composition of Functions

DEFINITION 29. Let X and Y be nonempty sets. We define $F(X,Y) = \{f \mid f\colon X \to Y\}$, the set of all functions from X to Y. If $X = Y$, we simply write $F(X)$.

DEFINITION 30 (Composition of functions). Let X, Y, Z be nonempty sets, and let $f\colon X \to Y$, $g\colon Y \to Z$. We define a function $g \circ f\colon X \to Z$, called the composition of f and g, by $g \circ f(x) = g(f(x))$, $\forall x \in X$.

REMARK 12. For the composition to be defined we just need the image of f to be a subset of the domain of g.

REMARK 13. In general, $g \circ f \neq f \circ g$! Give an example.

PROPOSITION 7. *Let $f\colon X \to Y$ be a function. Then $f \circ i_X = f$ and $i_Y \circ f = f$.*

PROOF. Hint: Use the definition of the composition and of the identity functions.

□

PROPOSITION 8 (Associativity of the composition). *Let $f\colon W \to X$, $g\colon X \to Y$, and $h\colon Y \to Z$. Then, $(h \circ g) \circ f = h \circ (g \circ f)$.*

PROOF. (Hint: Use the definition of the composition.)

□

EXERCISE 25. Let $f_1 \colon X_1 \to X_2$, $f_2 \colon X_2 \to X_3$, $f_3 \colon X_3 \to X_4$ and $f_4 \colon X_4 \to X_5$. Show that $((f_4 \circ f_3) \circ f_2) \circ f_1 = f_4 \circ (f_3 \circ (f_2 \circ f_1))$.

3. Surjective and Injective Functions

3.1. Definitions and examples.

DEFINITION 31 (Surjective function). A function $f \colon X \to Y$ is surjective (or onto, or a surjection) if every element in the codomain of f admits a preimage in the domain of f. Formally, $f \colon X \to Y$ is surjective if

$$(\forall y \in Y)(\exists x \in X)[y = f(x)].$$

PROPOSITION 9. *Let $f \colon X \to Y$ be a function. Then, f is surjective if and only if $\operatorname{Im}(f) = Y$.*

PROOF.

□

EXAMPLE 36. The identity function on X is surjective.

EXAMPLE 37. Let $f \colon (-\infty, 2) \cup (2, \infty) \to \mathbb{R}$, defined by $f(x) = \dfrac{3x+5}{x-2}$. The function f is not surjective since $\operatorname{Im}(f) = (-\infty, 3) \cup (3, \infty)$.

However, the function $g \colon (-\infty, 2) \cup (2, \infty) \to (-\infty, 3) \cup (3, \infty)$, defined by $g(x) = \dfrac{3x+5}{x-2}$ is surjective.

EXERCISE 26. Let $f \colon \mathbb{R} \to \mathbb{R}$, defined by $f(x) = x + 2|x|$. Is f surjective?

SOLUTION:

□

DEFINITION 32 (Injective function). A function $f\colon X \to Y$ is injective (or one-to-one, or an injection) if every two distinct elements in the domain have distinct images in the codomain. Formally, a function $f\colon X \to Y$ is injective if

$$(\forall x_1 \in X)(\forall x_2 \in X)[\neg(x_1 = x_2) \implies \neg(f(x_1) = f(x_2))].$$

REMARK 14. Using the contrapositive, a function f is injective if and only if

$$(\forall x_1 \in X)(\forall x_2 \in X)[(f(x_1) = f(x_2)) \implies (x_1 = x_2)].$$

EXAMPLE 38. The identity function on X is injective.

EXERCISE 27. Let $f\colon (-\infty, 2) \cup (2, \infty) \to \mathbb{R}$, defined by $f(x) = \dfrac{3x+5}{x-2}$. Is f injective?

SOLUTION:

□

EXERCISE 28. Let $f\colon \mathbb{R} \to \mathbb{R}$, defined by $f(x) = x + 2|x|$. Is f injective?

SOLUTION:

□

DEFINITION 33 (Bijective function). Let $f\colon X \to Y$ be a function. Then f is bijective (or a bijection) if f is both injective and surjective. In the case where $X = Y$ a bijection is simply called a permutation.

EXAMPLE 39.
(1) the identity function $i_X\colon X \to X$ is a permutation.
(2) the projections $\pi_X\colon X \times Y \to X, (x, y) \mapsto x$ and $\pi_Y\colon X \times Y \to Y, (x, y) \mapsto y$ are surjective.

EXERCISE 29. Let $f\colon (-\infty, 2) \cup (2, \infty) \to \mathbb{R}$, defined by $f(x) = \dfrac{3x+5}{x-2}$. Is f bijective?

SOLUTION:

□

3.2. Injectivity, surjectivity and composition.

THEOREM 15. *Let $f\colon W \to X$, $g\colon X \to Y$. If f and g are injective, then $g \circ f$ is also injective.*

PROOF. Assume that f and g are injective. Let $w_1, w_2 \in W$ such that $g \circ f(w_1) = g \circ f(w_2)$, then $g(f(w_1)) = g(f(w_2))$ (by definition of the composition) and $f(w_1) = f(w_2)$ (by injectivity of g). Now it follows from the injectivity of f that $w_1 = w_2$, and $g \circ f$ is injective.

□

EXERCISE 30. Let $f_1\colon X_1 \to X_2$, $f_2\colon X_2 \to X_3$, $f_3\colon X_3 \to X_4$ be three injective functions. Show that $f_3 \circ f_2 \circ f_1$ is injective.

SOLUTION:

□

THEOREM 16. *Let $f\colon W \to X$, $g\colon X \to Y$. If f and g are surjective, then $g \circ f$ is also surjective.*

PROOF. Assume that f and g are surjective. Let $y \in Y$, then there exists $x \in X$ such that $g(x) = y$ (by surjectivity of g). Since $x \in X$, there exists $w \in W$ such that $x = f(w)$ (by surjectivity of f). And hence, $y = g(x) = g(f(w)) = g \circ f(w)$ (by definition of the composition). We have just shown that for every $y \in Y$ there exists $w \in W$ such that $y = g \circ f(w)$, which means that $g \circ f$ is surjective. □

THEOREM 17. *Let $f\colon W \to X$, $g\colon X \to Y$. If f and g are bijective, then $g \circ f$ is also bijective.*

PROOF. Assume that f and g are bijective, then in particular they are both injective . By (2) $g \circ f$ is then injective. A similar reasoning using (3) will show that $g \circ f$ is surjective, an hence $g \circ f$ is bijective. □

THEOREM 18. *Let $f\colon W \to X$, $g\colon X \to Y$. If $g \circ f$ is injective, then f is injective.*

PROOF. Assume that $g \circ f$ is injective. Let $w_1, w_2 \in W$ such that $f(w_1) = f(w_2)$. Since g is a function one has $g(f(w_1)) = g(f(w_2))$ and $g \circ f(w_1) = g \circ f(w_2)$ (by definition of the composition). Since $g \circ f$ is injective it implies that $w_1 = w_2$, and f is injective. □

EXERCISE 31. Give sets X, Y, Z and functions $f\colon X \to Y$, $g\colon Y \to Z$ such that $g \circ f$ is injective, f is injective but g is not injective.

SOLUTION:

□

THEOREM 19. *Let $f\colon W \to X$, $g\colon X \to Y$. If $g \circ f$ is surjective, then g is surjective.*

PROOF.

□

4. Invertible Functions

DEFINITION 34. Let $f\colon X \to Y$ be a function. Then f is invertible if there is a function $g\colon Y \to X$ such that $f \circ g = i_Y$ and $g \circ f = i_X$.

EXERCISE 32. Let $f\colon X \to Y$ be a function. Assume that there are $g_1\colon Y \to X$ such that $f \circ g_1 = i_Y$ and $g_1 \circ f = i_X$ and $g_2\colon Y \to X$ such that $f \circ g_2 = i_Y$ and $g_2 \circ f = i_X$. Show that $g_1 = g_2$.

PROOF.

□

TERMINOLOGY. If f is invertible, the unique function satisfying the conditions of the previous definition is called the inverse of f and is denoted f^{-1}.

EXERCISE 33. Let $f\colon X \to Y$ and $g\colon Y \to Z$ be invertible functions. Show that $g \circ f$ is invertible.

PROOF.

□

THEOREM 20. *Let $f\colon X \to Y$. Then, f is invertible if and only if f is bijective.*

SKELETON OF THE PROOF.

- only if part: Assume f is invertible. Then, there exists $g\colon Y \to X$ such that $f \circ g = i_Y$ and $g \circ f = i_X$.
  - Injectivity: Let $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$.

    ...

    Then $x_1 = x_2$.
  - Surjectivity: Let $y \in Y$,

    ...

then $y = f(x)$ where $x = ... \in X$.

- if part: Assume that f is bijective, then f is injective, i.e. that $\forall x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$, then $x_1 = x_2$, and f is surjective, i.e. $\forall y \in Y, \exists x \in X$ such that $y = f(x)$.

  Define $g\colon Y \to X$ by $g(y) = ...$ Then, for all $y \in Y$

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

  and for all $x \in X$

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

□

5. Functions and Sets

Recall that the image of the function $f\colon X \to Y$ is the set $\mathrm{Im}(f) = \{y \in Y \mid (\exists x \in X)[y = f(x)]\}$. We generalize this concept in the following definition.

Definition 35 (Image of a set). Let $f\colon X \to Y$ be a function. If $Z \subseteq X$, the image of Z under f is the set, denoted $f(Z)$, of all elements in the codomain that are the image of an element in Z. Formally,

$$f(Z) = \{y \in Y \mid (\exists z \in Z)[y = f(z)]\}.$$

The image of f is simply $f(X)$, *i.e.,* $\mathrm{Im}(f) = f(X)$.

Proposition 10. *Let $f\colon X \to Y$ be a function. Let W and Z be subsets of X. If $W \subseteq Z$, then $f(W) \subseteq f(Z)$*

Proof.

□

Proposition 11. *Let $f\colon X \to Y$ be a function and W and Z be subsets of X. Then, $f(W \cap Z) \subseteq f(W) \cap f(Z)$*

Proof. Let $y \in f(W \cap Z)$, then there exists $x \in W \cap Z$ such that $y = f(x)$ (by definition of the image), thus $y = f(x)$ for some $x \in W$ and $y = f(x)$ for some $x \in Z$ (by definition of the intersection), and hence $y \in f(W)$ and $y \in f(Z)$ (by definition of the image), and $y \in f(W) \cap f(Z)$ (by definition of the intersection). Therefore $f(W \cap Z) \subseteq f(W) \cap f(Z)$. □

Proposition 12. *Let $f\colon X \to Y$ be a function and W and Z be subsets of X. Then, $f(W \cup Z) = f(W) \cup f(Z)$*

Proof. The proof is a classical double inclusion argument.

The inclusion $f(W \cup Z) \subseteq f(W) \cup f^{-1}(Z)$:
Let $y \in f(W \cup Z)$, then there exists $x \in W \cup Z$ such that $y = f(x)$ (by definition of the image) thus $y = f(x)$ for some $x \in W$ or $y = f(x)$ for some $x \in Z$ (by definition of the union) and hence $y \in f(W)$ or $y \in f(Z)$ (by definition of the image) and $y \in f(W) \cup f(Z)$ (by definition of the union). Therefore $f(W \cup Z) \subseteq f(W) \cup f(Z)$.

The inclusion $f(W) \cup f(Z) \subseteq f(W \cup Z)$:
Let $y \in f(W) \cup f(Z)$, then $y \in f(W)$ or $y \in f(Z)$ (by definition of the union) thus $y = f(x)$ for some $x \in W$ or $y = f(x)$ for some $x \in Z$ (by definition of the image) and $y = f(x)$ for some $x \in W \cup Z$ (by definition of the union) thus $y \in f(W \cup Z)$ (by definition of the inverse image). Therefore $f(W) \cup f(Z) \subseteq f(W \cup Z)$.

□

Definition 36. Let X and Y be nonempty sets and let $f\colon X \to Y$ be a function. Let Z be a subset of Y. Then the inverse image of Z with respect to the function f is the set $f^{-1}(Z) := \{x \in X \mid f(x) \in Z\}$.

Remark 15. In this context the symbol f^{-1} does not refer to the inverse of the function f.

Proposition 13. *Let X and Y be nonempty sets and let $f\colon X \to Y$ be a function. Let W and Z be subsets of Y. Then,*

(1) $f^{-1}(W \cup Z) = f^{-1}(W) \cup f^{-1}(Z)$
(2) $f^{-1}(W \cap Z) = f^{-1}(W) \cap f^{-1}(Z)$

Proof. (1) The proof is a classical double inclusion argument.

The inclusion $f^{-1}(W \cup Z) \subseteq f^{-1}(W) \cup f^{-1}(Z)$:
Let $x \in f^{-1}(W \cup Z)$, then $f(x) \in W \cup Z$ (by definition of the inverse image) thus $f(x) \in W$ or $f(x) \in Z$ (by definition of the union) and hence $x \in f^{-1}(W)$ or $x \in f^{-1}(Z)$ (by definition of the inverse image) and $x \in f^{-1}(W) \cup f^{-1}(Z)$ (by definition of the union). Therefore $f^{-1}(W \cup Z) \subseteq f^{-1}(W) \cup f^{-1}(Z)$.

The inclusion $f^{-1}(W) \cup f^{-1}(Z) \subseteq f^{-1}(W \cup Z)$:
Let $x \in f^{-1}(W) \cup f^{-1}(Z)$, then $x \in f^{-1}(W)$ or $x \in f^{-1}(Z)$ (by definition of the union) and $f(x) \in W$ or $f(x) \in Z$ (by definition of the inverse image) and hence $f(x) \in W \cup Z$ (by definition of the union) thus $x \in f^{-1}(W \cup Z)$ (by definition of the inverse image). Therefore $f^{-1}(W) \cup f^{-1}(Z) \subseteq f^{-1}(W \cup Z)$.

(2) The proof is a classical double inclusion argument.

The inclusion $f^{-1}(W \cap Z) \subseteq f^{-1}(W) \cap f^{-1}(Z)$:
Let $x \in f^{-1}(W \cap Z)$, then $f(x) \in W \cap Z$ (by definition of the inverse image) thus $f(x) \in W$ and $f(x) \in Z$ (by definition of the intersection) and hence $x \in f^{-1}(W)$ and $x \in f^{-1}(Z)$ (by definition of the inverse image) and $x \in f^{-1}(W) \cap f^{-1}(Z)$ (by definition of the intersection). Therefore $f^{-1}(W \cap Z) \subseteq f^{-1}(W) \cap f^{-1}(Z)$.

The inclusion $f^{-1}(W) \cap f^{-1}(Z) \subseteq f^{-1}(W \cap Z)$:
Let $x \in f^{-1}(W) \cap f^{-1}(Z)$, then $x \in f^{-1}(W)$ and $x \in f^{-1}(Z)$ (by definition of the intersection) and $f(x) \in W$ and $f(x) \in Z$ by definition of the inverse image, and hence $f(x) \in W \cap Z$ (by definition of the intersection) thus $x \in f^{-1}(W \cap Z)$ (by definition of the inverse

image). Therefore $f^{-1}(W) \cap f^{-1}(Z) \subseteq f^{-1}(W \cap Z)$.

□

6. Exercises

Exercise 34. Give an example of a function such that the inclusion is strict in Proposition 1.1. (3).

Exercise 35. Are the following functions injective, surjective, bijective?

(1) $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = 3x + 2$
(2) $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = \sin(2x)$
(3) $f\colon \mathbb{R} \to [-1, 1]$, $f(x) = \cos(5x)$
(4) $f\colon \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, $f(n) = (n, n)$

Exercise 36. Let f and g two permutations of X. Show that $g \circ f$ is a permutation of X as well.

Exercise 37. Let X and Y be nonempty sets, and $f\colon X \to Y$ be a function. Suppose that f has a right inverse h; that is, there exists a function $h\colon Y \to X$ such that $f \circ h = i_Y$. Prove that f is surjective.

Solution. Let $y \in Y$, then

$$\begin{aligned} y &= i_Y(y) \text{ (by definition of the identity function on } Y) \\ &= f \circ h(y) \text{ (since } f \circ h(y) = i_Y(y) \text{ by definition of } h \text{ being a right inverse of } f) \\ &= f(h(y)) \text{ (by definition of the composition).} \end{aligned}$$

If we let $x = h(y)$ then $x \in X$ (since the codomain of h is X) and $y = f(x)$. We just proved that for all $y \in Y$, there is $x \in X$ such that $y = f(x)$, which means that f is surjective. □

Exercise 38. Let X and Y be nonempty sets, and $f\colon X \to Y$ be an injective function. Let A be a subset of X. Prove that $f^{-1}(f(A)) = A$.

Solution. The result is proved by a double inclusion argument. We first prove that $f^{-1}(f(A)) \subseteq A$. Let $x \in f^{-1}(f(A))$, then $f(x) \in f(A)$ (by definition of the inverse image of a subset), and there exists $a \in A$ such that $f(x) = f(a)$ (by definition of the image of a subset). Since f is injective it follows that $x = a$, and hence $x \in A$ (because $a \in A$).

We now prove that $A \subseteq f^{-1}(f(A))$. Let $x \in A$, then $f(x) \in f(A)$ (by definition of the image of a subset) and $x \in f^{-1}(f(A))$ (by definition of the inverse image of a subset).

□

Exercise 39. Let X and Y be nonempty sets, and $f\colon X \to Y$ be an surjective function. Let A be a subset of Y. Prove that $f(f^{-1}(A)) = A$.

Solution. The result is proved by a double inclusion argument. We first prove that $f(f^{-1}(A)) \subseteq A$. Let $y \in f(f^{-1}(A))$, then $y = f(x)$ for some $x \in f^{-1}(A)$ (by definition of the image), and $f(x) \in A$ (by definition of the inverse image). But $y = f(x)$ belongs to A since $f(x)$ does. Therefore $f^{-1}(f(A)) \subseteq A$.

We now prove that $A \subseteq f(f^{-1}(A))$. Let $a \in A$, then $a \in Y$ since A is a subset of Y. By surjectivity of f, there exists $x \in X$ such that $a = f(x)$, and $f(x) \in A$ (since a is in A). It follows that $x \in f^{-1}(A)$ (by definition of the inverse image) and $f(x) \in f(f^{-1}(A))$ (by definition of the image). Therefore $a \in f(f^{-1}(A))$. □

CHAPTER 6

Relations

1. Definitions and basic properties

DEFINITION 37. Let X and Y be sets. A relation R from X to Y is a subset of $X \times Y$. If $(x, y) \in R$ we simply write xRy. We simply say that R is a relation on X if it is a relation from X to X. In other words, a relation R on a set X is a subset of $X \times X$

EXAMPLE 40.
(1) Let $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid y = kx, \text{ for some } k \in \mathbb{Z}\}$. Then $2R4$, $19R0$...
(2) Let R on $\mathbb{Z}$ such that $xRy \iff x - y = 5k$ for some $k \in \mathbb{Z}$.
(3) Let R on $F(\mathbb{R})$ such that $fRg \iff f(0) = g(0)$.
(4) let R on $P(X)$ such that $ARB \iff A \subseteq B$.
(5) let R on $P(X)$ such that $ARB \iff A \subset B$.

DEFINITION 38 (Reflexivity). A relation R on a set X is reflexive if every element in X is in relation with itself. Formally, R is reflexive if

$$(\forall x \in X)\ xRx.$$

DEFINITION 39 (Symmetry). A relation R on a set X is symmetric if for all elements $x, y \in X$ such that x is in relation with y then y is in relation with x. Formally, R is symmetric if

$$(\forall x \in X)(\forall y \in X)[xRy \implies yRx].$$

DEFINITION 40 (Transitivity). A R be a relation on a set X is transitive if for all elements $x, y, z \in X$ such that x is in relation with y and if y is in relation with z, then x is in relation with z. Formally, R is transitive if

$$(\forall x \in X)(\forall y \in X)(\forall z \in X)[((xRy) \wedge (yRz)) \implies (xRz)].$$

2. Equivalence relations and partitions

DEFINITION 41 (Equivalence relation). A relation R on a set X is an equivalence relation if it is reflexive, symmetric and transitive.

For an equivalent relation R, xRy is often denoted by $x \sim y$ and reads x equivalent to y.

DEFINITION 42. If $\sim$ is an equivalence relation on X, and $x \in X$, the set $[x] = \{y \in X \mid y \sim x\}$ is called the equivalence class of x. Elements of the same class are said to be equivalent.

The purpose of defining an equivalence relation is to classify elements of a set according to a certain property. As we will see having an equivalence relation provides a procedure to partition a set. We now introduce the concept of a partition. Let Y be a set and $\mathcal{P}$ a subset of $P(Y)$. We use the notation $\bigcup_{A \in \mathcal{P}} A$ for $\bigcup_{A \in \mathcal{P}} X_A$ where $X_A = A$. In other words, the set $\bigcup_{A \in \mathcal{P}} A$ is the set of all elements that belong to at least one set of $\mathcal{P}$.

DEFINITION 43 (Partition). Let X be a set. A partition of X is a subset $\mathcal{P}$ of $P(X)$ such that

(1) $\bigcup_{A\in\mathcal{P}} A = X$, (covering)
(2) if $A, B \in \mathcal{P}$ and $A \neq B$, then $A \cap B = \emptyset$, (disjointness)
(3) if $A \in \mathcal{P}$ then $A \neq \emptyset$. (non-empty clucters)

THEOREM 21. *If $\sim$ is an equivalence relation on a nonempty set X, then the set of equivalence classes of $\sim$ forms a partition of X.*

PROOF. Uses reflexivity and transitivity of the equivalence relation. □

THEOREM 22. *Let $\mathcal{P}$ be a partition of a nonempty set X. Define a relation $\sim_{\mathcal{P}}$ on X by $x \sim_{\mathcal{P}} y$ if and only if x and y are in the same element of the partition. Then $\sim_{\mathcal{P}}$ is an equivalence relation on X.*

PROOF. Definition based direct proof. □