MATH 215: LECTURE 3- BASIC SET THEORY

TOM BENHAMOU
UNIVERSITY OF ILLINOIS AT CHICAGO

Set theory is the basic mathematical theory which is commonly accepted as the language to describe the mathematical universe.

1. SETS

We will focus on the so-called "näive" set theory (rather than axiomatic set theory) where the notion of a set is not explicitly defined. Instead we will give rules of thumb to describe sets and how to imagine and handle them.

Definition 1.1. A *set* is a collection of mathematical objects without repetitions and without ordering.

To understand this definition better, let us jump directly to the description of sets and through the example we will understand it better. In general, there are exactly three ways to define a set.

1.1. The list principle.

$$\{a, b, c, ..., z\},\ \{1, 5, 17\},\ \{\{1, 2\}, \{2, 3\}\}$$

A set is always denoted with curly brackets $\{,\}$. Between the brackets we specify the *members* or *elements* of the set separated by commas.

Let us denote the set of *natural numbers* by:

$$\mathbb{N} = \{0, 1, 2, ...\}$$

Definition 1.2. The membership relation $a \in A$ is the statement that the object a is a member of the set A

Example 1.3. $1 \in \{1\}, \{2, 2\} \in \{\{1\}, \{2\}\}, \{3\} \notin \{3, 4, 5\}, \{1, 10, 100\} \ni 1, \frac{1}{2} \notin \mathbb{N}$

Formally, we can define the "List Principle" by

$$a \in \{a_1, ..., a_n\} \equiv a = a_1 \vee a = a_2 ... \vee a = a_n$$

Remark 1.4.
(1) To explain the fact that sets have no order, we note that the sets $\{1, 2, 3\}, \{2, 3, 1\}$ represent the same set.
(2) To explain the fact that sets have no repetitions, we note that $\{1, 1, 2, 3\}, \{1, 2, 3\}$ represent the same set.

Date: August 19, 2022.

(3) Bounded quantifiers: it will be convenient to use the notion of quantifiers which are bounded in a given set A:

$$\forall x \in A.p(x) \equiv \forall x.x \in A \to p(x)$$
$$\exists x \in A.p(x) \equiv \exists x.x \in A \wedge p(x)$$

We think of these quantifiers as quatifiters which range over a given set.

Remember: The membership relation is always between a member of a set and a set

1.2. **The separation principle.** Given a set A an a predicate $p(x)$ where x is a free variable in the set A, we can *separate* from A the elements $a \in A$ which satisfy $p(a)$ into a new set. This separated set is denoted by:

$$\{x \in A \mid p(x)\}$$

This reads as "the set of all x in A such that $p(x)$ holds true".

Example 1.5. (1) $\{x \in \{1,2,6,7\} \mid x > 3\} = \{6,7\}$

(2) $p(x)$ is the predicate $\exists k \in \mathbb{N}(3 \cdot k = x)$. Then we can separate from $\mathbb{N}$ the following set:

$$\{x \in \mathbb{N} \mid \exists k \in \mathbb{N}(3 \cdot k = x)\} = \{0,3,6,9,....\}$$

(3) $A = \{1,3,6,11,21,17\}$, $\{x \in A \mid x+1 \textit{ is prime}\} = \{1,6\}$

(4) $B = \{\{1\},\{2\},\mathbb{N},\{\mathbb{N}\},\{x \in \mathbb{N} \mid x \cdot x = x\}\}$

$$\{x \in B \mid 1 \notin x\} = \{\{2\},\{\mathbb{N}\}\}$$

Define $a \in \{x \in A \mid p(x)\} \equiv a \in A \wedge p(a)$

1.3. **The replacement principle.** Let A be a set and $f(x)$ some operation/ function on the elements of A. We can *replace* every memeber a of the set A by the outcome of the operation $f(a)$ and collect all the outcomes into a new set. This new collection is denoted by:

$$\{f(x) \mid x \in A\}$$

This reads as "the set of all outcomes $f(x)$ where the parameter x runs in the set A".

Example 1.6.

- $f(x) = 2^x$, $\{2^x \mid x \in \mathbb{N}\} = \{2^0, 2^1, 2^2, ...\} = \{1,2,4,8,16,....\}$
- $\{\{x\} \mid x \in \{1,4,3\}\} = \{\{1\},\{3\},\{4\}\}$. Sets of the form $\{a\}$ are called *singletons*.
- $\{x+1 \mid x \in \mathbb{N}\} = \{x \in \mathbb{N} \mid x > 0\}$

Define $a \in \{f(x) \mid x \in A\} \equiv \exists x \in A.f(x) = a$

Important: a formula of the form $a \in A$ is a **statement** and should be proven by the definitions given above for each of the three principles.

Exercise 1. *Prove the following membership statements:*

(1) $2 + 5 \in \{1,2,...,10\}$.

Proof. By the list principle, we need to prove that

$$(2+5=1) \vee (2+5=2) \vee ... \vee (2+5=10)$$

Indeed, $2+5=7$ hence the $\vee$-statement holds. □

(2) $5 \in \{x \in \mathbb{N} \mid \exists y \in \mathbb{Z}.y + x = 5\}$.

Proof. By the separation principle, we need to prove that $5 \in \mathbb{N} \wedge \exists y \in \mathbb{Z}.y + 5 = 5$. This is a $\wedge$-statement, so we need to prove two parts:

(a) $5 \in \mathbb{N}$, this is clear by the definition of the natural numbers.
(b) We need to prove that $\exists y \in \mathbb{Z}.y + 5 = 5$. Define $y = 0$, then $y \in \mathbb{Z}$ and $y + 5 = 0 + 5 = 5$.

□

(3) $\{1\} \in \{\{n, 1\} \mid n \in \mathbb{N}\}$.

Proof. By the replacement principle, we need to prove that $\exists n \in \mathbb{N}.\{1\} = \{1, n\}$. Define $n = 1$, indeed $1 \in \mathbb{N}$ and since there are no repetitions in sets we have that

$$\{1, n\} = \{1, 1\} = \{1\}.$$

□

2. Famous sets

(1) $\mathbb{N} = \{0, 1, 2, 3, ...\}$ you will not need to explain basic properties of the natural numbers which relates to addition, multiplication and power of natural numbers. Here are some other properties we assume about the natural numbers:
   - Every natural number has an immediate successor.
   - The natural numbers are *well-ordered*, which simply says that every set of natural numbers (finite or infinite) has a minimal element.
   - Every finite set of natural numbers has a maximal element.
(2) The set of positive natural numbers is: $\mathbb{N}_+ = \{x \in \mathbb{N} \mid x > 0\} = \{1, 2, 3, 4, ...\}$
(3) The set of integers is: $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$
(4) The set of fractions/ rational numbers is: $\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z} \wedge n \neq 0\}$
(5) The set of real numbers is denoted by $\mathbb{R}$. We wont formally define the reals. We will simply describe them as numbers which have a (possibly infinite) decimal representation such as: 15.6755897847566372..... Among the real numbers, one can find $\sqrt{2}, \pi, e$. One of the most important properties of the reals is that the rational numbers are dense inside them:

$$\forall r_1, r_2 \in \mathbb{R}.r_1 < r_2 \Rightarrow (\exists q \in \mathbb{Q}.r_1 < q < r_2)$$
$$\mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}.$$

(6) The intervals:

- $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$ denotes the *open interval* between a and b.
- $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$ the *closed interval*.
- $[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\}$. Define similarly $(a, b]$.
- $(a, \infty) = \{x \in \mathbb{R} \mid a < x\}$ is the *infinite ray*. Similarly define $[a, \infty), (-\infty, a), (-\infty, a]$. Note that $(a, \infty]$ is not defined since ∞ is not a natural number.

(7) $\emptyset$ denoted the empty set, which is characterized by the following property: $\forall x.x \notin \emptyset$. Namely, the empty set is a set with no element. It is sometimes convenient to think of $\emptyset = \{\}$.

3. Inclusion and the extensionality principle

Definition 3.1. Let A, B be any sets. We say that A *is included in* B and denote it by $A \subseteq B$ if

$$\forall x.x \in A \Rightarrow x \in B$$

In other words, if every element of A is an element of B. Using bounded quantifiers we can say that $A \subseteq B$ is the statement $\forall x \in A.x \in B$.

Example 3.2. $\{1, 5\} \subseteq \mathbb{N}_{odd} \subseteq \mathbb{N}_+ \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

3.1. **Proving sets inclusion.** Since $A \subseteq B$ is a universal implication, we have the following format:

(1) The proof starts with "Let $a \in A$".
(2) Then we should deduce from the assumption of that $a \in A$ usually that requires to interpret that assumption that $a \in A$. that $a \in B$ and the proof should terminate by "$a \in B$".

Of course, in special cases we can use the other methods of proving universal statements (such as proving $a \in B$ going over $a \in A$ one-by-one)

Example 3.3. Prove the following inclusions:

(1) $\{2, -1\} \subseteq \{x \in \mathbb{Z} \mid x^2 > x\}$.

Proof. Let $a \in \{2, -1\}$. Since $\{2, -1\}$ includes only two elements, let us prove that $a \in B$ by going over the elements of $\{2, -1\}$ one-by-one:

(a) For $a = 2$, we need to prove that $2 \in \{x \in \mathbb{Z} \mid x^2 > x\}$. By the separation principle we need to prove that $2 \in \mathbb{Z} \wedge 2^2 > 2$. Indeed 2 is an integer and $2^2 = 4 > 2$.
(b) For $a = -1$, we need to prove that $-1 \in \mathbb{Z} \wedge (-1)^2 > -1$. Indeed, -1 is an integer and $(-1)^2 = 1 > -1$.

□

(2) $\{n^2 + n \mid n \in \mathbb{N}\} \subseteq \mathbb{N}_{even}$.

Proof. Let $x \in \{n^2 + n \mid n \in \mathbb{N}\}$. We need to prove that $x \in \mathbb{N}_{even}$. By the replacement principle, there exist $n \in \mathbb{N}$ such that $x = n^2 + n$, so let $n_0 \in \mathbb{N}$ be such that $x = n_0^2 + n_0$. In is an easy exercise to deduce now that x is even, namely that $x \in \mathbb{N}_{even}$. □

(3) For every $a, b, c \in \mathbb{R}$. If $a < b < c$, then there is $\epsilon > 0$ such that $(a, b+\epsilon] \subseteq (a, c)$.

Proof. Let $a, b, c \in \mathbb{R}$ such that $a < b < c$. We need to prove that there is $\epsilon > 0$ such that $(a, b+\epsilon] \subseteq (a, c)$A moment of reflection reviles that we only need to find $0 < \epsilon$ such that $b + \epsilon < c$, hence $0 < \epsilon < c - b$. The following definition of ϵ is tailored to satisfy exactly these inequalities.. Define $\epsilon = \frac{c-b}{2}$. Since $c > b$, we have that $c - b > 0$ and also $\epsilon = \frac{c-b}{2} > 0$. Let us prove that[1] $(a, b+\epsilon] \subseteq (a, c)$. This is an inclusion, let $x \in (a, b+\epsilon]$. By definition of intervals, this means that $x \in \mathbb{R} \wedge (a < x \leq b+\epsilon)$. We need to prove that $x \in (a, c)$, namely, that $x \in \mathbb{R} \wedge (a < x < c)$. Indeed by the assumption, $x \in \mathbb{R}$, and $a < x$. To see that $x < c$, we use the definition of ϵ:

$$x \leq b + \epsilon = b + \frac{c-b}{2} < b + (c - b) = c$$

Hence $a < x < c$ and we conclude that $x \in (a, c)$. □

Problem 1. *Prove that if $A \subseteq B \wedge B \subseteq C$, then $A \subseteq C$.*

Theorem 3.4. *For every set A, $\emptyset \subseteq A$.*

Proof. [2] Let A be a set. We need to prove that $\emptyset \subseteq A$. Note here the assumption "Let $a \in \emptyset$" is impossible. Instead, we recall that in order to prove that $\emptyset \subseteq A$ we need to prove that $\forall x. x \in \emptyset \Rightarrow x \in A$. Let x be any element, then $x \in \emptyset$ is false by the definition of $\emptyset$ and therefore the implication $x \in \emptyset \Rightarrow x \in A$ is vacuously true. □

Definition 3.5. We denote by $A \nsubseteq B$ if $\neg(A \subseteq B)$, namely, if $\exists x \in A. x \notin B$.

Example 3.6. Prove that $\{n \in \mathbb{N} \mid n^2 - 7n + 12 = 0\} \nsubseteq \mathbb{N}_{odd}$

Proof. For example[3] $4 \notin \mathbb{N}_{odd}$ and also $4 \in \{n \in \mathbb{N} \mid n^2 - 7n + 12\}$, since $4 \in \mathbb{N}$ and $4^2 - 7 \cdot 4 + 12 = 0$. □

3.2. **Set equality.** The extensionality principle is a basic principle (axiom) in set theory which expresses the fact the a set is determined by its elements.

Definition 3.7. The extesionality principle is the fact that for any two sets A, B:

$$A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$$

This means that when we wish to prove set equality $A = B$, we do so by proving a *double inclusion*:

(1) Prove $A \subseteq B$.
(2) Prove $B \subseteq A$.

[1] Recall that to prove an existential statement we give the example and prove it satisfy the desired property.

[2] Here is and example for the 0.1% of the cases where we prove that an implication is vacuously true.

[3] We need to prove an existential statement so we provide an example.

Example 3.8. Prove that $\mathbb{N}_+ = \{x \in \mathbb{Z} \mid \exists y \in \mathbb{N}.y + 1 = x\}$.

Proof. Let us denote the set of the right-hand side by A. We want to prove $\mathbb{N}_+ = A$. This is sets equality and we prove it by a double inclusion:

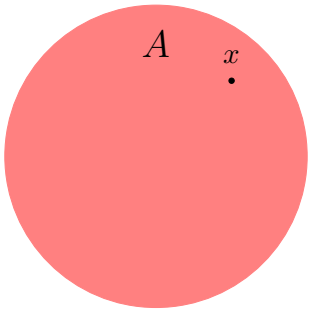
(1) $\mathbb{N}_+ \subseteq A$: Let $n_0 \in \mathbb{N}^+$, then $n_0 \geq 1$ is an integer. We want to prove that $n_0 \in A$, by the separation principle, we want to prove that $n_0 \in \mathbb{Z} \wedge \exists y \in \mathbb{N}.y + 1 = n_0$. Clearly, $n_0 \in \mathbb{Z}$. Define $y = n_0 - 1$. Note that $y \geq 0$ is an integer, hence $y \in \mathbb{N}$ and clearly $y + 1 = n_0$, hence $n_0 \in A$.

(2) $A \subseteq \mathbb{N}_+$: Let $a_0 \in A$. We want to show that $a_0 \in \mathbb{N}_+$. By the separation principle, we know that $a_0 \in \mathbb{Z}$ and that $\exists y \in \mathbb{N}.y + 1 = a_0$. Let $y_0 \in \mathbb{N}$ witness that $y_0 + 1 = a_0$. Since $y_0 \in \mathbb{N}$, we have that $y_0 \geq 0$ and therefore $a_0 = y_0 + 1 \geq 1$. It follows that $a_0 \in \mathbb{N}_+$.

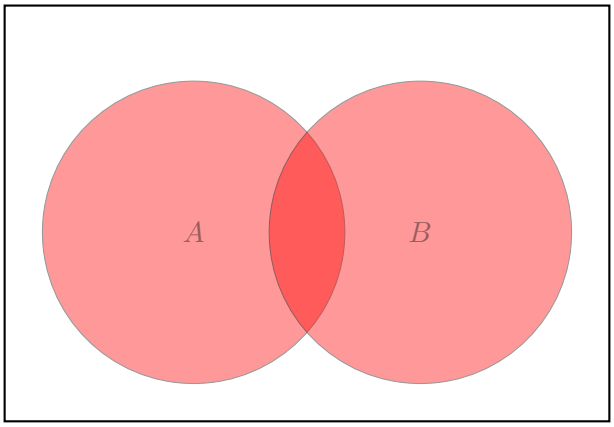
□

4. Venn Diagram and set operations

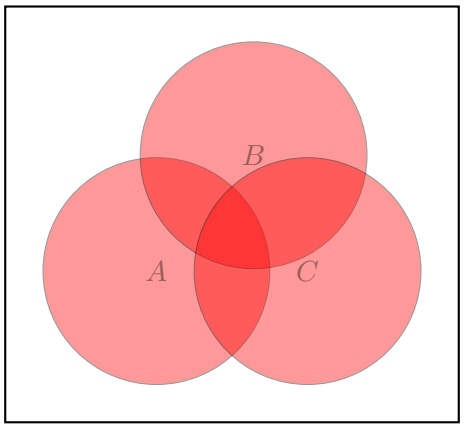
The graphical way to imagine sets and elements it to think of a set A as an area and a member of it $x \in A$ as a point in that area:



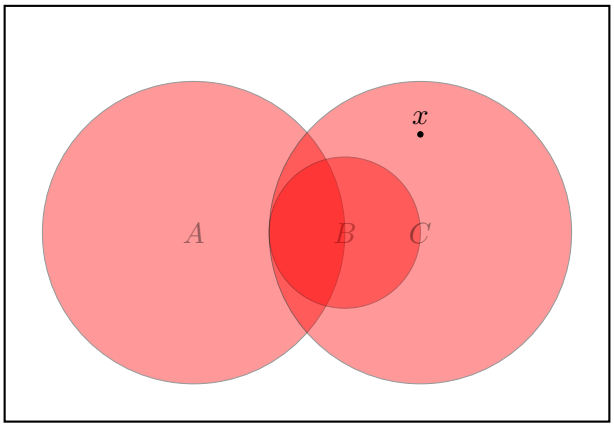
A Venn diagram of two or more sets, is graphial representation of general sets.



Three sets:



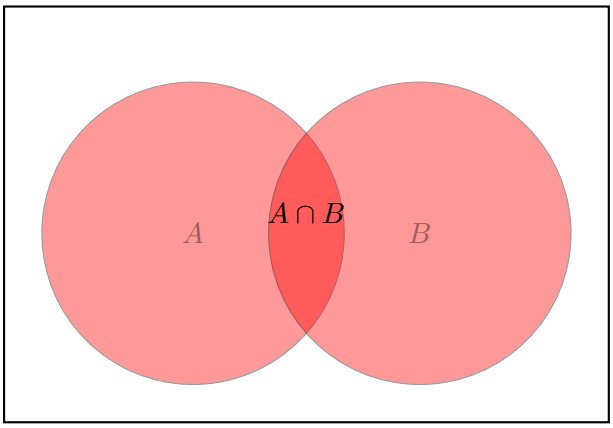
We can also add extra assumption to the diagram, for example if $B \subsetneq C$ we can express it as follows:



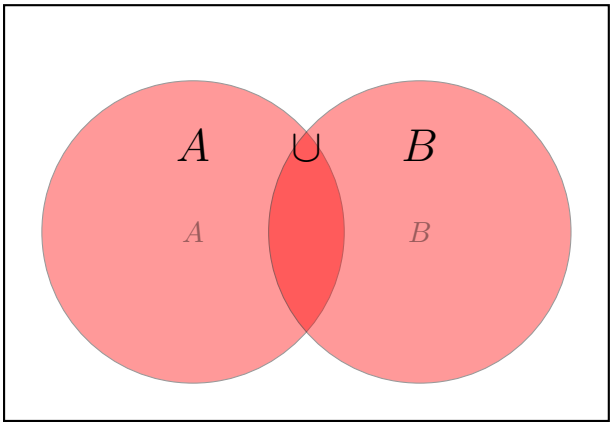
Note that x is a witness for a member of B which is not in C. A vigilant reader will notice that the picture is not fully accurate as we do not know if the witness x belongs to A.

Definition 4.1. Let A, B be sets

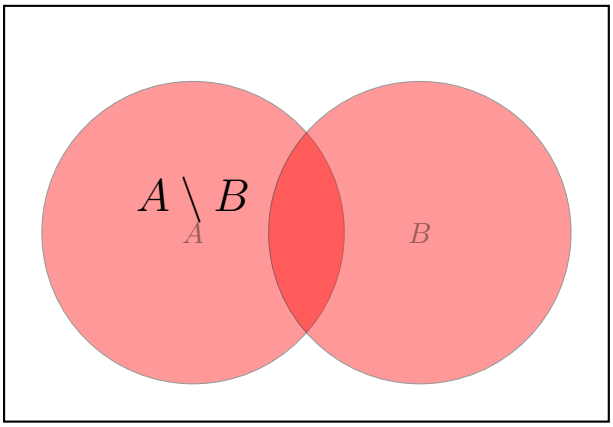
(1) The *intersection* of the sets is defined by $A \cap B = \{x \mid x \in A \wedge x \in B\}$.



(2) The *union* of the two sets is denoted by $A \cup B = \{x \mid x \in A \vee x \in B\}$

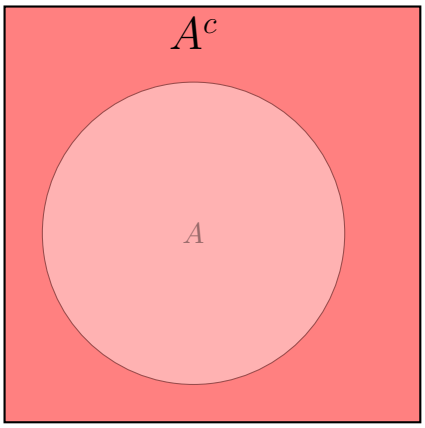


(3) The *difference* of the sets is defined by $A \setminus B = \{x \in A \mid x \notin B\}$

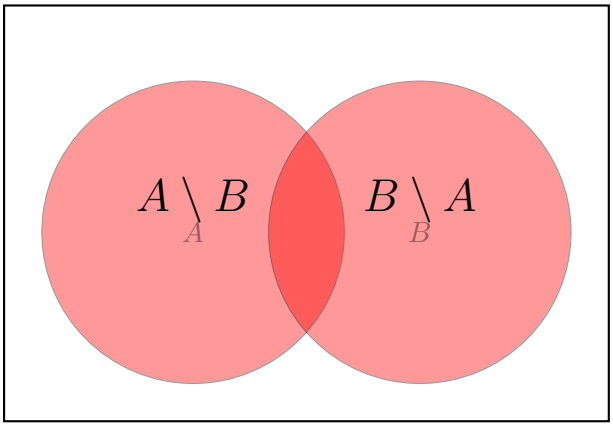


In the literature, difference of sets is sometimes denoted by $A - B$.

(4) The *complement* of A inside a supset U of A is denoted by $A^c = U \setminus A$. This is conceptually different from difference since we assume that U is some framework set and then A^c is an operation on a single set.



(5) The *symmetric difference* of the sets is denoted by $A\Delta B = (A \setminus B) \cup (B \setminus A)$



Example 4.2. (1) $\{1,2\} \cup \{2,3\} = \{1,2,3\}$, $\{1,4,5\} \cap \{2,4,4\} = \{4\}$, $[0,\infty) \cap (-\infty,1) = [0,1)$

(2) $\{1,2,6\} \setminus \{2,7,8\} = \{1,6\}$, $A \cap A = A \cup A = A$, the set of irrational numbers is the set $\mathbb{R} \setminus \mathbb{Q}$

Proposition 4.3. *Sets operations identities:*

(1) Associativity:
- *(a)* $A \cap (B \cap C) = (A \cap B) \cap C$.
- *(b)* $A \cup (B \cup C) = (A \cup B) \cup C$.
- *(c)* $A\Delta(B\Delta C) = (A\Delta B)\Delta C$.

(2) Commutativity:
- *(a)* $A \cap B = B \cap A$.
- *(b)* $A \cup B = B \cup A$.
- *(c)* $A\Delta B = B\Delta A$.

(3) Distributivity:
- *(a)* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
- *(b)* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

(4) Identities of difference and De-Morgan low's for sets:

(a) $A \setminus B = A \cap B^c$.
(b) $(A \cup B)^c = A^c \cap B^c$.
(c) $(A \cap B)^c = A^c \cup B^c$.
(d) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
(e) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

(5) *Identities of the empty set:*
(a) $A \cap \emptyset = \emptyset$.
(b) $A \cup \emptyset = A$.
(c) $A \setminus \emptyset = A$.
(d) $\emptyset \setminus A = \emptyset$.
(e) $A \Delta \emptyset = A$.

(6) *Identities of a set and itself:*
(a) $A \cap A = A$.
(b) $A \cup A = A$.
(c) $A \setminus A = \emptyset$.
(d) $A \Delta A = \emptyset$.

As examples, we will prove some of the items. We encourage the readers to write the proof for the other items.

Proof of 3.(b). We need to prove sets equality. We do so by proving a double inclusion.

$\underline{(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)}$: Let $x \in (A \cap B) \cup (A \cap C)$. By definition of $\cup$, we can split into cases:

(1) If $x \in A \cap B$, then by definition of $\cap$, $x \in A \wedge x \in B$. Hence $x \in B \cup C$ and $x \in A \cap (B \cup C)$.
(2) If $x \in A \cap C$ then $x \in A \wedge x \in C$. Once again, $x \in B \cup C$, thus $x \in A \cap (B \cup C)$.

In both cases we conclude that $x \in A \cap (B \cup C)$.

$\underline{(A \cap B) \cup (A \cap C) \supseteq A \cap (B \cup C)}$: Exercise.

□

Proof of 4.(e). Let us prove it using the other items.

$$A \setminus (B \cup C) \overset{4.(a)}{=} A \cap (B \cup C)^c \overset{4.(b)}{=} A \cap (B^c \cap C^c) \overset{6.(a)}{=} (A \cap A) \cap (B^c \cap C^c) =$$

$$\overset{2.(a)+1.(a)}{=} (A \cap B^c) \cap (A \cap C^c) \overset{4.(a)}{=} (A \setminus B) \cap (A \setminus C)$$

□

Proposition 4.4. *The following are equivalent:*

(1) $A \subseteq B$
(2) $A \cap B = A$
(3) $A \setminus B = \emptyset$
(4) $A \cup B = B$

Proof. We shall prove: (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1).[4]

(1) $\Rightarrow$ (2): Suppose $A \subseteq B$. We need to prove that $A \cap B = A$. We need to prove a double inclusion: Clearly, $A \cap B \subseteq A$. As for the other inclusion, let $x \in A$, since $A \subseteq B$ we conclude $x \in B$ and therefore $x \in A \cap B$ thus $A = A \cap B$.

(2) $\Rightarrow$ (3): Suppose that $A \cap B = A$ and suppose toward a contradiction that $AB \neq \emptyset$. By the definition of $\emptyset$, we conclude that there is $x \in A \setminus B$. By definition of sets difference, $x \in A \wedge x \notin B$. By definition of $\cap$, $x \notin A \cap B$. Thus $x \in A$ and $x \notin A \cap B$. By extensionality, $A \neq A \cap B$, contradicting the assumption.

(3) $\Rightarrow$ (4) and (4) $\Rightarrow$ (1) are left as exercises.

□

5. The power set

Definition 5.1. Let A be any set. define the *power set* of A as the set f all possible subsets of A. We denote it by

$$P(A) = \{x \mid x \subseteq A\}$$

Example 5.2. (1) $P(\{0,1\}) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$
(2) $P(\{\{1\}, 2\}) = \{\emptyset, \{\{1\}\}.\{2\}, \{\{1\}, 2\}\}$
(3) $\emptyset, A \in P(A)$

Problem 2. *$A \subseteq B$ If and only if $P(A) \subseteq P(B)$.*

Proof. $\Rightarrow$: Suppose that $A \subseteq B$. We want to prove that $P(A) \subseteq P(B)$. To prove the inclusion, let $X \in P(A)$, we want to prove that $X \in P(B)$. By definition of power set, $X \in P(A)$ implies that $X \subseteq A$. By the assumption $A \subseteq B$ and by a transitivity of inclusion we conclude that $X \subseteq B$. Again by definition of the power set, we have that $X \in P(B)$.

$\Leftarrow$: Suppose that $P(A) \subseteq P(B)$. We want to prove that $A \subseteq B$. Usually, we would take an element $a \in A$ and try to prove that $a \in B$. However, there is a "trick" here which simplifies the proof. We have that $A \in P(A)$ and by the assumption, $P(A) \subseteq P(B)$, hence $A \in P(B)$. By definition of power set this means that $A \subseteq B$, as wanted. □

Definition 5.3. For a finite set A, we denote be $|A|$ the number of elements in the set A. For example $|\{1,2,3,18,-3\}| = 5$ and $|(-5,5) \cap \mathbb{Z}| = 9$.

Theorem 5.4. *Let A be a finite set then $|P(A)| = 2^{|A|}$.*

"Proof". Suppose that $A = \{a_1, ..., a_n\}$.

Every subset $X \subseteq A$, defines a sequence of n yes/no answers in the following way: for each $i = 1, ..., n$, we ask the question, is $a_i \in X$? For example suppose that:

[4]This is a standard trick to prove equivalence between several statements. The order is not important as long as we close a circle of implications.

- a_1 yes
- a_2 no
- a_3 no
- $a_4, ..., a_n$ yes

Then the sequence of answers would be

$$yes, no, no, yes, yes, yes, ..., yes$$

Note that from this sequence of answers we can reproduce the subset $X = \{a_1, a_4, ..., a_n\}$. This means that we are left to count the number of possible sequences of answers. Since typically there are n answers, with 2 possibilities for each answer we conclude that there are

$$\underbrace{2 \cdot 2....2}_{ntimes} = 2^n$$

many subsets of A. □

Problem 3. *What is the sequence of answers which corresponds to $\emptyset, A$?*

5.1. **Ordered pairs and Cartesian product.** Many mathematical objects involve order and repetitions. For example, the coordinates of a point in the plane is an object for which the order is important (since the point $P = (1, 2)$ is not the same point as $Q = (2, 1)$) and repetition is allowed (there is the point $(1, 1)$). Let us define using sets, objects which allow order and repetition:

Definition 5.5. Let x, y be two objects, the *ordered pair* of x and y is defined by $\langle x, y\rangle = \{\{x\}, \{x, y\}\}$.

Example 5.6.

The basic property of pairs is the following property for which we omit the proof:

Claim 5.6.1. *For every a, b, c, d*

$$\langle a, b\rangle = \langle c, d\rangle \Leftrightarrow a = c \wedge b = d$$

Definition 5.7. Let A, B be two sets. The *Cartesian product* of the sets (named after René Descartes) is defined by $A \times B = \{\langle a, b\rangle \mid a \in A, B \in B\}$

Also define the *square* of a set A is to be $A \times A$.

Example 5.8.
(1) $\{1, 2\} \times \{3, 4\} = \{\langle 1, 3\rangle, \langle 1, 4\rangle, \langle 2, 3\rangle, \langle 2, 4\rangle\}$
(2) $\{2, 3\}^2 = \{\langle 2, 2\rangle, \langle 2, 3\rangle, \langle 3, 2\rangle, \langle 3, 3\rangle\}$
(3) The *Real plane* is defined to be the set $\mathbb{R}^2$.

6. Induction and Recursion

Induction and recursion and extremely related techniques, however, they have totally different purposes:

Important Induction is a proof technique while **Recursion** is a definition technique.

6.1. **Recursion.** As we said, recursion is a definition technique, but what does it define? sequences:

Definition 6.1. A *sequence* of elements of a set A is an list of elements of A enumerated by the natural numbers.[5]

Example 6.2. The following are examples of sequences:

(1) The sequence $a_n = n$ is the sequence $0, 1, 2, 3, 4, ...$
(2) The sequence $b_n = \frac{1}{n+1}$ is the sequence $1, \frac{1}{2}, \frac{1}{3}, ...$
(3) The sequence $c_n = (-1)^n$ is the sequence $1, -1, 1, -1, 1, ...$
(4) The sequence d_n of the sum of angles in degrees of a polygon with $n+3$ vertexes, is the sequence $180^o, 360^o, 540^o, ...$ and actually $d_n = (n+1) \cdot 180^o$.

Definition 6.3. A *recursive* definition of a sequence has two parts:

(1) Initial values of the sequence: A definition of the first few values of the sequence.
(2) The recursive condition: A formula to compute the next element in the sequence from the previous elements.

Remark 6.4. The number of previous elements required to define the next element is called the *depth* of the recursion. The depth of the recursion determined how many initial values should we specify.

(1) $a_0 = 0$, $a_{n+1} = a_n + 1$, the depth is 1.
(2) An arithmetic sequence is a sequence of the form $a_0 = a$ and $a_{n+1} = a_n + d$, for some given a, d. For example: $a_0 = 5$ and $a_{n+1} = a_n - 7$.
(3) A geometric sequence is a sequence of the form $a_0 = a$ and $a_{n+1} = a_n \cdot q$ for some given a, q for example $a_0 = 5$ and $a_{n+1} = a_n \cdot (-7)$.
(4) $a_0 = a_1 = 1$ and $a_{n+1} = a_n + a_{n-1}$. Here the depth is 2. This is called the Fibonacci sequence.
(5) $0! = 1$ and $(n+1)! = n! \cdot (n+1)$.
(6) $a_1 = \emptyset$ and $a_{n+1} = \{a_n\}$. We are allowed to start the enumeration from a natural number grater than 0.

Definition 6.5. Let us define by recursion an n-tuple. A 1-tuple is defined by $\langle a \rangle = a$. Given we have defined an n-tuple, we define $n+1$-tuples using n-tuples and ordered pairs we have already defined.:

$$\langle a_1, ..., a_n, a_{n+1} \rangle = \langle \langle a_1, ...a_n \rangle, a_{n+1} \rangle$$

Example 6.6. (1) $\langle a_0 \rangle = a_0$.

(2) Note that a 2-tuple is the same as an ordered pairs. Indeed, let us denote momentarily the 2-tuple by $\langle a_0, a_1 \rangle^*$, then we have

$$\langle a_0, a_1 \rangle^* = \langle \langle a_0 \rangle, a_1 \rangle = \langle a_0, a_1 \rangle$$

.

[5]The real definition of a sequence involves the concept of functions which we will study later.

(3) $\langle a_0, a_1, a_2\rangle = \langle\langle a_0, a_1\rangle, a_2\rangle =$

$\{\{\langle a_0, a_1\rangle\}, \{\langle a_0, a_1\rangle, a_2\}\} = \{\{\{\{a_0\}, \{a_0, a_1\}\}\}, \{\{\{a_0\}, \{a_0, a_1\}\}, a_2\}\}$

(4) $\langle a_0, a_1, a_2, a_3\rangle = \langle\langle\langle a_0, a_1\rangle, a_2\rangle, a_3\rangle$

6.2. **induction.** One of the most common techniques for proving **Universal statements** of the form $\forall n \in \mathbb{N}$... is a proof by induction. Let us explain our goal and the idea behind induction.

Suppose we would like to prove a claim of the form

"For every **natural number** n, q(n) (some property of n)"

This is extremely important that the statement speaks about natural numbers. In order to prove such statement, we can use a proof by induction. The point is to prove an infinite chain of implications:

$$q(0) \Rightarrow q(1) \Rightarrow q(2) \Rightarrow ...q(n) \Rightarrow q(n+1) \Rightarrow ...$$

This is done by proving **for a general** n that $q(n) \Rightarrow q(n+1)$, this is called *the inductive step*. Then the final step is to prove $q(0)$ which is called the *base of the induction*. If we proved both the base of the induction and the induction step then we can now derive the property for every natural number since:

- $q(0)$ is true by the base.
- $q(0) \Rightarrow q(1)$, then $q(1)$ is true.
- $q(1) \Rightarrow q(2)$, then $q(2)$ is true, and so on.

Practically, since $q(n) \Rightarrow q(n+1)$ is a universal implication, a *proof by induction* for the claim $\forall n \in \mathbb{N}.q(n)$ has the following structure:

(1) The base of the induction: Proof for $q(0)$.
(2) Induction hypothesis: "Suppose that $q(n)$ holds", here n is a general variable.
(3) Induction step: We need to prove that $q(n+1)$ holds, under the given induction assumption that $q(n)$ holds.

Example 6.7. Prove by induction the following claims:

(1) $\forall n \in \mathbb{N}.n^2 \geq n$.

Proof. **The induction base:** We need to prove that for $n = 0$, $0^2 \geq 0$, this is indeed true since $0^2 = 0$.

The induction hypothesis(Abbreviated I.H.): Let n be any natural number, and suppose that $n^2 \geq n$.

The induction step: We need to prove that $(n+1)^2 \geq n+1$. Indeed,

$$(n+1)^2 = n^2 + 2n + 1 \underbrace{\geq}_{\text{Since } n \geq 0} n^2 + 1 \underbrace{\geq}_{I.H.} n + 1$$

□

(2) $\forall n \geq 1(n+1 \leq 2n)$. We can start the induction from a natural number greater than 0, this only changes the base of the induction.

Proof. **The induction base:** We need to prove the claim for $n = 1$. Indeed,

$$1 + 1 = 2 \leq 2 = 2 \cdot 1$$

The induction Hypothesis: Suppose that for a general $n \geq 1$, $n + 1 \leq 2n$.

The induction step: We need to prove that $(n+1)+1 \leq 2(n+1)$. Indeed,

$$(n + 1) + 1 \underset{I.H}{\leq} 2n + 1 \leq 2n + 2 = 2 \cdot (n + 1)$$

□

(3) $\forall n > 3.2^n < n!$.

Proof. **The induction base:** We need to prove the claim for $n = 4$, indeed $2^4 = 16 \leq 24 = 4!$.

The induction hypothesis: Suppose that for a general $n > 3$, $2^n < n!$.

The induction step: We need to prove that $2^{n+1} < (n + 1)!$. Indeed,

$$2^{n+1} = 2^n \cdot 2 \underset{I.H.}{\leq} n! \cdot 2 \underset{\text{Since } n>3}{\leq} n! \cdot (n + 1) \underset{\text{Recursive def}}{=} (n + 1)!$$

□

(4) A general term for an arithmetic sequence. Suppose that $a_n = a_{n-1} + d$ is an arithmetic sequence. Then for every $n \in \mathbb{N}$, $a_n = a_0 + d \cdot n$. (homework: geometric sequence and sum of squares)

Proof. **The induction base:** For $n = 0$, we need to prove that $a_0 = a_0 + d \cdot 0$. This is clearly true.

The induction hypothesis: Suppose that for a general n, $a_n = a_0 + dn$.

The induction step: We need to prove that $a_{n+1} = a_0 + d(n+1)$. Using the recursive definition of a_n, we have that:

$$a_{n+1} = a_n + d \underset{I.H.}{=} a_0 + dn + d = a_0 + d(n + 1)$$

□

(5) The partial sum of a arithmetic sequence. Suppose that $a_n = a_{n-1} + d$ is an arithmetic sequence. Then for every $N \in \mathbb{N}$,

$$\sum_{i=0}^{N} a_i = a_0 + a_1 + ... + a_N = (N + 1)(a_0 + dN/2)$$

Proof. **The induction base:** We need to prove the formula for $N = 0$, $a_0 = (0 + 1)(a_0 + d \cdot 0/2)$. This is clear.

The induction hypothesis: Suppose that the formula is true for a general N, namely, we assume that truth of the equality

$$\sum_{i=0}^{N} a_i = a_0 + a_1 + ... + a_N = (N+1)(a_0 + dN/2)$$

The induction step:

$$\sum_{i=0}^{N+1} a_i = \underbrace{a_0 + ... + a_N}_{\sum_{i=0}^{N} a_i} + a_{N+1} \underset{I.H.}{=} (N+1)(a_0 + dN/2) + a_{N+1} \underset{\text{Previous exercise}}{=}$$

$$= (N+1)(a_0 + dN/2) + a_0 + d(N+1) = (N+2)a_n + (N+1)d(N/2+1) =$$
$$(N+2)a_0 + (N+2)d(N+1)/2 = (N+2)(a_0 + d(N+1)/2)$$

□

For example, consider the arithmetic sequence $a_n = n$ (here $a_0 = 0$ and $d = 1$) then we can apply the formula to conclude that

$$0 + 1 + 2 + ... + 1000 = 1001(0 + 1 \cdot 1000/2) = 1001 \cdot 500 = 500,500$$

(6) Prove that for any given n lines in the plane, no two are parallel, and no three intersect at a single point[6], have exactly $\frac{n(n-1)}{2}$ points of intersection. (homework: the sum of angles of a polygon)

Proof. Let d_n denote the number of intersection points of n non-concurrent lines. We firs construct a recursive formula for d_n. Clearly, $d_1 = 0$ (and $d_2 = 1$, $d_3 = 3$). Given n non-concurrent lines, they have d_n intersection points. Adjoining a new line to them, it intersect each of the lines exactly once (since it is not parallel to any of them) and the points of intersection are different since no three lines intersect at a point. Hence

$$d_{n+1} = \underbrace{d_n}_{\text{The intesection points of the old lines}} + \underbrace{n}_{\text{the intersections with the new line}}$$

Now let us prove by induction that $d_n = \frac{n(n-1)}{2}$.

The induction base: Indeed $d_1 = 0 = \frac{0 \cdot (-1)}{2}$.

The induction hypothesis: Suppose that for a general n, $d_n = \frac{n(n-1)}{2}$.

The induction step: We need to prove that $d_n = \frac{(n+1)n}{2}$. We use the recursive description of d_{n+1},

$$d_{n+1} = d_n + n = \frac{n(n-1)}{2} + n = n(\frac{n-1}{2} + 1) = n\frac{n-1+2}{2} = \frac{n(n+1)}{2}$$

□

(7) Define the recursive sequence $a_0 = \emptyset$, $a_{n+1} = P(a_n)$. Then for every $n \in \mathbb{N}$, $a_n \subseteq a_{n+1}$.

[6]Such lines are called *non-concurrent* lines.

Proof. **The induction base:** For $n = 0$ we need to prove that $a_0 \subseteq a_1$. By definition $a_0 = \emptyset$, and we have already prove that the empty set is included in every set. In particular $a_0 = \emptyset \subseteq a_1$.

The induction hypothesis: Suppose that for a general n, $a_n \subseteq a_{n+1}$.

The induction step: We need to prove that $a_{n+1} \subseteq a_{n+2}$. This is an inclusion proof, so let $X \in a_{n+1}$. We need to prove that $X \in a_{n+2}$. By definition, $a_{n+1} = P(a_n)$, and by the assumption, $X \in P(a_n)$. By definition of the power set, $X \subseteq a_n$. By the induction hypothesis, $a_n \subseteq a_{n+1}$. We already saw that if $a \subseteq b \wedge b \subseteq c$ then $a \subseteq c$. It our case, we conclude that $X \subseteq a_{n+1}$. Again by the definition of the power set, $X \in P(a_{n+1}) = a_{n+2}$, as wanted.

□

(8) For all $n \in \mathbb{N}_+$ and $a_1, .., a_n, b_1, .., b_n$,

$$\langle a_1, .., a_n\rangle = \langle b_1, ..., b_n\rangle \Longleftrightarrow \forall 1 \leq i \leq n.a_i = b_i$$

Proof. We will use Claim 5.6.1, that for every a_1, a_2, b_1, b_2

$$\langle a_1, a_2\rangle = \langle b_1, b_2\rangle \Leftrightarrow a_1 = b_1 \wedge a_2 = b_2$$

The induction is of the variable n, which is the length of the n-tuple.

The induction base: For $n = 1$, we need to prove that for every a_1, b_1

$$(\star) \quad \langle a_1\rangle = \langle b_1\rangle \Longleftrightarrow a_1 = b_1$$

Recall that by definition of 1-tuple, $\langle a\rangle = a$, hence the equivalence $(\star)$ is clear.

The induction hypothesis: Suppose that for a general n, for every $a_1, .., a_n, b_1, ..., b_n$,

$$\langle a_1, .., a_n\rangle = \langle b_1, ..., b_n\rangle \Longleftrightarrow \forall 1 \leq i \leq n.a_i = b_i$$

The induction step: We need to prove that for every $a_1, .., a_{n+1}, b_1, ..., b_{n+1}$,

$$\langle a_1, .., a_{n+1}\rangle = \langle b_1, ..., b_{n+1}\rangle \Longleftrightarrow \forall 1 \leq i \leq n+1.a_i = b_i$$

Let $a_1, ..., a_{n+1}, b_1, ..., b_{n+1}$. We need t prove that

$$\langle a_1, .., a_{n+1}\rangle = \langle b_1, ..., b_{n+1}\rangle \Longleftrightarrow \forall 1 \leq i \leq n+1.a_i = b_i$$

We will prove this equivalences with a chain of equivalences which we already know.

$$\langle a_1, .., a_{n+1}\rangle = \langle b_1, ..., b_{n+1}\rangle \underset{\text{Recursive definition of } n\text{-tuples}}{\Longleftrightarrow} \langle\langle a_1, .., a_n\rangle, a_{n+1}\rangle = \langle\langle b_1, ..., b_n\rangle, b_{n+1}\rangle$$

$$\underset{\text{Pairs equality}}{\Longleftrightarrow} \langle a_1, .., a_n\rangle = \langle b_1, ..., b_n\rangle \wedge a_{n+1} = b_{n+1} \underset{\text{I.H.}}{\Longleftrightarrow}$$

$$\forall 1 \leq i \leq n.a_i = b_i \wedge a_{n+1} = b_{n+1} \Longleftrightarrow \forall 1 \leq i \leq n+1.a_i = b_i$$

□