Elementary Set Theory and Logic

Cezar Ionescu

WS 2023-24

Sets

Sets are the most fundamental objects of mathematics. As such, it is impossible to give a definition in terms of “simpler” objects. As Halmos says (Halmos 2017)

> [We assume] that the reader has the ordinary, human, intuitive (and frequently erroneous) understanding of what sets are; the purpose of this exposition is to delineate some of the many things one can correctly do with them.

Notation 1.

- Let S be a set. We write $x \in S$ to denote that x is an **element** of S, and $x \notin S$ to denote that x is *not* an element of S.
- Let S and T be sets. We write $T \subseteq S$ to denote that T is a **subset** of S, i.e., every element of T is also an element of S.
- Let S be a set and x_1, x_2, ..., x_n be elements of S. Then $\{x_1, x_2, \ldots, x_n\}$ denotes the set that comprises exactly these elements (*enumeration notation*).
- Let S be a set and P a family of statements indexed with elements from S. Then $\{x \mid x \in S,\ P(x)\}$ denotes the subset of elements of S having the property P. This notation is called **set comprehension**.

Remark 1. The set comprehension is used only to select subsets of a given set. Unrestrictive use leads to confusion. Consider the **Russell set**:

$$R = \{\text{sets } S \mid S \notin S\}$$

and the question whether $R \in R$ or not.

Notation 2. We shall use the following notation for important sets:

1. The **empty set** will be denoted by $\emptyset$
2. The set of **natural numbers** will be denoted by $\mathbb{N}$:

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

3. The set of **integers** will be denoted by $\mathbb{Z}$:

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

4. The set of **rational numbers** will be denoted by $\mathbb{Q}$:

$$\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z}, n > 0\}$$

5. The set of **real numbers** will be denoted by $\mathbb{R}$. It contains all the numbers with a decimal expansion.

6. The set of **complex numbers** will be denoted by $\mathbb{C}$:

$$\mathbb{C} = \{x + yi \mid x, y \in \mathbb{R}\}$$

   where $i = \sqrt{-1}$.

7. Let $a, b \in \mathbb{R}$. **Intervals** will be denoted by

$$\begin{aligned}
(a, b) &= \{x \in \mathbb{R} \mid a < x < b\} \\
[a, b) &= \{x \in \mathbb{R} \mid a \leq x < b\} \\
(a, b] &= \{x \in \mathbb{R} \mid a < x \leq b\} \\
[a, b] &= \{x \in \mathbb{R} \mid a \leq x \leq b\} \\
(a, \infty) &= \{x \in \mathbb{R} \mid a < x\} \\
[a, \infty) &= \{x \in \mathbb{R} \mid a \leq x\} \\
(-\infty, b] &= \{x \in \mathbb{R} \mid x \leq b\} \\
(-\infty, b) &= \{x \in \mathbb{R} \mid x < b\}
\end{aligned}$$

Remark 2.
- For any set S, we have $\emptyset \subseteq S$
- We have $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Elementary Logic

Propositional logic

Notation 3. Let P and Q denote logical statements such as $x \geq y$ or "there exists a z, such that $z^2 < 0$".

1. $P \land Q$ denotes the logical statement P *and* Q (that is, both P and Q are true)
2. $P \lor Q$ denotes the logical statement P *or* Q (at least one of P and Q is true)
3. $P \Rightarrow Q$ denotes the logical statement P *implies* Q (if P is true, then Q is also true)

4. $P \iff Q$ denotes the logical statement P *is equivalent to* Q, or P *if and only if* Q (P and Q are either both true, or both false).

5. $\neg P$ denotes the logical statement *not* P (if P is true, then $\neg P$ is false, and the other way around).

The truth conditions given above is usually summarized using **truth tables**.

P	Q	P ∧ Q
F	F	F
F	T	F
T	F	F
T	T	T

P	Q	P ∨ Q
F	F	F
F	T	T
T	F	T
T	T	T

P	¬P
F	T
T	F

P	Q	P $\Rightarrow$ Q
F	F	T
F	T	T
T	F	F
T	T	T

P	Q	P $\iff$ Q
F	F	T
F	T	F
T	F	F
T	T	T

The meaning of the logical operations allows us to prove logical statements such as the following.

Proposition 1. Let P and Q denote logical statements. Then the logical statement $(P \wedge Q) \Rightarrow P$ is true.

Proof. To show that $(P \wedge Q) \Rightarrow P$ is true, we must show that **if** $P \wedge Q$ is true, **then** Q is true. But if $P \wedge Q$ is true, then both P and Q must be true, therefore P must be true. □

We can also use truth tables to prove such statements. For example, the following truth table shows that $(P \wedge Q) \Rightarrow P$ is always true:

P	Q	P ∧ Q	(P ∧ Q) ⇒ P
F	F	F	T
F	T	F	T
T	F	F	T
T	T	T	T

Definition 1. A statement that is always true, independent of the truth values of its components, is called a **tautology**.

Example 1. The following are tautologies:

- $P \vee \neg P$ (**law of excluded middle**)
- $\neg\neg P \Leftrightarrow P$ (**law of double negation**)
- $\neg(P \wedge \neg P)$ (**law of contradiction**)
- $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$ (**modus ponens**)

Quantifiers

Let $P(x)$ be a familiy of logical statements indexed on the elements of a set S, for example $x \geq 0$ for elements in $S = \mathbb{N}$.

Notation 4. 1. The symbol $\forall$ denotes the **universal quantifier** "for all". The statement $\forall x \in S \bullet P(x)$ is true if and only if the statement $P(x)$ is true for every $x \in S$.

2. The symbol $\exists$ denotes the **existential quantifier** "there exists". The statement $\exists x \in S \bullet P(x)$ is true if and only if there exists an element $a \in S$ such that $P(a)$ is true.

Remark 3. Note that you must always provide the set S on which the statement P is indexed! For example, $\forall x \in \mathbb{N} \bullet x \geq 0$ is true, but $\forall x \in \mathbb{Z} \bullet x \geq 0$ is false.

Remark 4. The order of quantifiers is important! For example, the following statements are not at all equivalent:

$$\forall x \in S \bullet \exists y \in T \bullet P(x, y)$$
$$\exists y \in T \bullet \forall x \in S \bullet P(x, y)$$

For example, let $S = T = \mathbb{N}$ and $P(x, y)$ be the statement $x \leq y$. Then the first statement says that for any natural number we can always find a bigger one, while the second one states that there is a greatest natural number.

Proposition 2. (De Morgan's Laws for quantifiers) Let $P(x)$ be a family of statements indexed by the elements x of some set S. Then

$$\neg(\forall x \in S \bullet P(x)) \iff \exists x \in S \bullet \neg P(x)$$
$$\neg(\exists x \in S \bullet P(x)) \iff \forall x \in S \bullet \neg P(x)$$

The proof follows from the meaning of quantifiers.

Definition 2. (Vacuously true statement) Whatever the family of statements $P(x)$, the statement $\exists x \in \emptyset \bullet P(x)$ is always false (since no such x can exist). Therefore the statement

$$\neg(\exists x \in \emptyset \bullet P(x)) \iff \forall x \in \emptyset \bullet \neg P(x)$$

is always true. A statement of the form

$$\forall x \in \emptyset \bullet P(x)$$

is called **vacuously true**, and is always true.

Operations on sets

In what follows, let X and Y be subsets of a set S.

Using elementary logic, we can give a formal definition of set equality and inclusion.

Definition 3.

1. $X = Y \iff \forall x \in S \bullet (x \in X \iff x \in Y)$
2. $X \subseteq Y = \iff \forall x \in S \bullet (x \in X \Rightarrow x \in Y)$

It follows that

Proposition 3.

$$X = Y \iff (X \subseteq Y \wedge Y \subseteq X)$$

Definition 4. (Operations on sets)

1. **union**
$$X \cup Y = \{x \mid x \in S,\ x \in X \vee x \in Y\}$$
2. **intersection**
$$X \cap Y = \{x \mid x \in S,\ x \in X \wedge x \in Y\}$$
3. **difference**
$$X \setminus Y = \{x \mid x \in S,\ x \in X \wedge x \notin Y\}$$
4. **complement**
$$X^c = \{x \mid x \in S\ ,\ x \notin X\}$$
5. **symmetric difference**
$$X \Delta Y = X \setminus Y \cup Y \setminus X$$
6. **power set**
$$\mathcal{P}(X) = \{Y \mid Y \subseteq X\}$$

   Alternatively:

$$Y \in \mathcal{P}(X) \iff Y \subseteq X$$

7. **cartesian product**

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

8. **disjoint union**

$$X \sqcup Y = \{(x, 0) \mid x \in X\} \ \cup\ \{(y, 1) \mid y \in Y\}$$

Sets as Building Blocks

All the operations we have so far need some pre-existing sets to operate on, but all we need to get started is the empty set $\{\}$ or $\emptyset$, and we can create a universe of sets that can be used to represent all mathematical objects that we need.

For example: the natural numbers. We can use the set $\emptyset$ to stand for zero, this will be our first natural number. So $0 = \emptyset$. Then, we could take:

- $1 = \{\emptyset\}$, that is, 1 has one element, namely the empty set. Note that this means that 1 is not the same set as 0, since 1 has an element, and 0 has none!
- $2 = \{1\}$, that is, 2 also has only one element, the number 1. 2 is different from 1, because while both have one element each, the two elements are different in each case.
- $3 = \{2\}$, and so on. In general, we'll have

$$n + 1 = \{n\}$$

This is *recursive definition*. We have a starting point, $0 = \emptyset$, and a recursive clause, $n+1 = \{n\}$ which allows us to determine the set representation of any natural number. Conversely, if we are given a set representing a natural number, we can determine what natural number that is. We can even determine if a given set represents or not a given number, by the following algorithm:

- Is the set empty? If yes, it represents the number 0.
- If not, does the set contain more than one element? If so, then it does not represent any natural number.
- If not, then it must have exactly one element, and the answer is determined by applying the algorithm to it.

There is problem here: the algorithm only terminates if there does not exist a set consisting just of layers and layers going on forever

$$\{\{\ldots\{\{\{\ldots\}\}\}\ldots\}\}$$

In standard set theory, the *axiom of foundation* precludes the existence of such a set.

We can add two "numbers" by a similar recursive procedure:

- $\emptyset + n = n$

- $(m + 1) + n = \{m + n\}$

You should convince yourselves that this is correct.

This is not the only way to represent the natural numbers, and is in fact not even the most commonly used one, which was developed by John von Neumann (so these sets are known as *von Neumann numbers*).

The von Neumann numbers are:

- $0 = \emptyset$
- $n + 1 = n \cup n$

Exercise 1. Write the von Neumann representation for 1, 2, and 3.

In this fashion, the number n is represented by a set with exactly n elements. It is also easy to compare two such numbers for inequality:

$$m \leq n \iff m \subseteq n$$

Addition is not much simpler to define, though:

- $0 + n = n$
- $(m + 1) + n = (m + n) \cup \{m + n\}$

Exercise 2. Carry out the following additions using both representations of natural numbers:

- $1 + 1$
- $2 + 2$
- $3 + 1$

It doesn't matter which representation we choose. In either case, the natural numbers will obey the same fundamental properties: addition will be associative and commutative, we will be able to define a corresponding multiplication, and results will always turn out the same. The only difference will be in the answers to "spurious" questions such as "What is the powerset of 10?".

The existence of more than one satisfactory representation is a situation common in computer science. A data structure such as an array or a stack can be implemented in many different ways. Even machine integers can look differently on different machines, depending on whether a "big-endian" or a "little-endian" representation is used (in a "big-endian" system, the numbers are read from left to right, as we are used to). In computer science, the essential properties that have to be preserved by all implementations form the *specification* of the data structure. In mathematics, the essential properties are usually given by *axioms*. Axiomatic definitions are older than computer science and have had an important influence on the development of the concepts of specification and correctness of programs.

Binary Relations

Definition 5. Let A and B be subsets of a given set S. A **binary relation** between elements of A and B is a subset of the set $A \times B$.

If $A = B$, then the relation is called **relation on** A.

If $R \subseteq A \times B$ is a relation, we will also write $x\ R\ y$ instead of $(x, y) \in R$.

Definition 6.
- The **domain** of a binary relation $R \subseteq A \times B$ is the set

$$\text{dom}(R) = \{x | x \in A, \exists y \in B \bullet (x, y) \in R\}$$

- The **range** of a binary relation $R \subseteq A \times B$ is the set

$$\text{ran}(R) = \{y | y \in B, \exists x \in A \bullet (x, y) \in R\}$$

Definition 7. The **composition** of two relations $R_1 \subseteq A \times B$ and $R_2 \subseteq B \times C$ is

$$R_1 \circ R_2 = \{(x, z) \mid x \in A,\ y \in B,\ z \in C,\ xR_1y \wedge yR_2z\} \subseteq A \times C$$

Definition 8. The **converse** of a binary relation $R \subseteq A \times B$ is a relation $R^\circ \subseteq B \times A$ such that

$$R^\circ = \{(y, x) \mid x \in A,\ y \in B,\ (x, y) \in R\}$$

Remark 5.

$$\text{dom}(R^\circ) = \text{ran}(R), \quad \text{ran}(R^\circ) = \text{dom}(R)$$

Definition 9. **(Properties of relations)** Let A be a set, and R a relation on A. Then

1. R is **reflexive** if $\forall x \in A \bullet xRx$
2. R is **anti-reflexive** if $\forall x \in A \bullet \neg xRx$
3. R is **symmetric** if $\forall x, y \in A \bullet xRy \Rightarrow yRx$
4. R is **anti-symmetric** if $\forall x, y \in A \bullet xRy \wedge yRx \Rightarrow x = y$
5. R is **transitive** if $\forall x, y, z \in A \bullet (xRy \wedge yRz) \Rightarrow xRz$

Definition 10. **(Special relations)** Let A be a set, and R a relation on A.

1. R is a **partial order** on A if R is reflexive, anti-symmetric, and transitive.
2. R is a **total order** (or just **order**) on A if R is a partial order and, additionally, $\forall x, y \in A \bullet xRy \vee yRx$.
3. R is a **partial strict order** on A if R is anti-reflexive and transitive.
4. R is a **total strict order** on A if R is a partial strict order and, additionally, $\forall x, y \in A \bullet xRy \vee yRy \vee x = y$.

5. R is an **equivalence relation** if R is reflexive, symmetric, and transitive.

Example 2.

1. $<$ is not a partial order on $\mathbb{R}$.
2. $\leq$ is a (total) order on $\mathbb{R}$.
3. $\subseteq$ is a partial order on $\mathcal{P}(A)$.
4. None of the previous examples is an equivalence relation.
5. Let A be the set of cars at a given dealership. The relation R on A defined by xRy if x and y have the same price is an equivalence relation on A.
6. The **identity relation** on A, id_A, defined by $xid_Ay \Leftrightarrow x = y$, is an equivalence relation.

Proposition 4. If R_1 and R_2 are reflexive (symmetric, transitive) relations on A, then $R_1 \cup R_2$ is also a reflexive (symmetric, transitive) relation on A.

Definition 11. Given an equivalence relation R on a set A and $a \in A$, the **equivalence class** of a with respect to R is

$$[a]_R = \{x \mid x \in A, xRa\}$$

If the relation R is clear from context, we omit the subscript $_R$ (and refer to the *equivalence class* of a).

Example 3. Given $n \in \mathbb{N}_{\geq 2}$, the relation $\equiv_n$ (*equivalence modulo* n) on $\mathbb{Z}$ is defined by

$$x \equiv_n y \quad \Leftrightarrow \quad x \mod n = y \mod n$$

This relation is an equivalence relation. The equivalence classes are given by the possible rests when dividing by n, so each of $[0]$, $[1]$, ..., $[n-1]$ is a distinct equivalence class and their union is the entire set of integers, $\mathbb{Z}$.

Example 4. The relation D on $\mathbb{N} \times \mathbb{N}$ defined by

$$(x_1,\ y_1)\ D\ (x_2,\ y_2) \quad \Leftrightarrow \quad x_1 + y_2 = x_2 + y_1$$

is an equivalence relation

Proposition 5. In any equivalence class of D there is a unique element $(x,\ y)$ satisfying $x = 0 \vee y = 0$.

Definition 12.

1. The set of *integers* is defined as the set of equivalence classes of D:

$$\mathbb{Z} = \{[(x, y)]_D \mid x \in \mathbb{N}, y \in \mathbb{N}\}$$

2. We use the notation:
   - $0 := [(0, 0)]_D$

- $n := [(n, 0)]_D$
- $-n := [(0, n)]_D,$ if $n > 0$

3. The *addition* operation on integers is defined by

$$[(x_1, y_1)]_D + [(x_2, y_2)]_D = [(x_1 + x_2, y_1 + y_2)]_D$$

Example 5. Check that $5 - 3 = 2$ and $3 - 5 = -2$.

References

- *Naive Set Theory*, Paul Halmos, Dover 2017 (reprint of 1960 edition published by D. Van Nostrand)
- *Introduction to University Mathematics*, Richard Earl, Michelmas 2020, unpublished lecture notes.