CHAPTER 1

Sets (section 3.1)

1.1. Introduction

Problem p 161
Goal:

- Introduce the formalism of set theory
- Use it to solve counting problems

1.2. Sets and basic manipulations of sets

1.2.1. Definition.

DÉFINITION. A *set* A is a collection of objects.

Defining property: you can ask whether an object a belongs to A or not.
Objects or elements: $a, b, c, ...$
Sets: $A, B, C, ...$
Predicates:

- $a \in S$: a belongs to S, or a is an element of S, or S contains a;
- $a \notin S$: a does not belong to S.

Two sets A and B are *equal* $(A = B)$ if they contain the same elements:

$$(\forall x)(x \in A) \Leftrightarrow (x \in B)$$

1.2.2. How to define a set S? You have to describe which elements are in the set S and which are not.

- List the elements of the set S:

  $$S := \{a, b, c\}$$

  $a \in S$ is true, whereas $d \in S$ is false.
  The order and the repetition are irrelevant:

  $$\{a, b, c\} = \{a, b, b, b, c\} = \{c, b, a\}$$

  Note that a and $\{a\}$ are two different things. The first is the object a, whereas the second one is the set containing a, and no other elements.
- Provide a predicate which determines which element are in S:

  $$S := \{x \mid P(x)\}$$

  $$S := \{x \mid x \text{ is an integer and } 3 < x \leq 7\}$$

  $5 \in S$ is true, whereas $3 \notin S$, and no car belongs to A.

- Use a *recursive definition*, as for the set of well formed formulas:
  S contains basic propositions $A, B, C, ...$
  If P and Q belong to S, then P', $P \wedge Q$, $P \vee Q$, $P \to Q$, $P \leftrightarrow Q$ also belong to S.

Some usual sets:

- The empty set:
$$\emptyset := \{x \,|\, false\}$$
- Numbers:
$$\mathbb{N} := \{x \,|\, x \text{ is a non negative integer }\}$$
$$\mathbb{Z} := \{x \,|\, x \text{ is an integer }\}$$
$$\mathbb{Q} := \{x \,|\, x \text{ is a rational number }\}$$
$$\mathbb{R} := \{x \,|\, x \text{ is a real number }\}$$
$$\mathbb{C} := \{x \,|\, x \text{ is a complex number }\}$$
$$S^* := \{x \,|\, x \in S \text{ and } x \neq 0\}$$
$$S^+ := \{x \,|\, x \in S \text{ and } x \geq 0\}$$

1.2.3. Relationships between sets.

- A is a *subset* of B ($A \subseteq B$) iff any element of A is in B:
$$(\forall x)(x \in A) \Rightarrow (x \in B)$$
- A is a *proper subset* of B ($A \subset B$) iff A is a subset of B but they are not equal :
$$(\forall x)(x \in A) \Rightarrow (x \in B) \text{ and } (\exists x)(x \in B) \wedge (x \notin A)$$

Exercice 1. [**?**, Exercise 10 p. 117]
$$R := \{1, 3, \pi, 4, 1, 9, 10\},\ S := \{\{1\}, 3, 9, 10\}$$

$$T := \{1, 3, \pi\},\ U := \{\{1, 3, \pi\}, 1\}$$

(1) $S \subseteq R$?
(2) $1 \in R$?
(3) $1 \in S$?
(4) $1 \subseteq U$?
(5) $\{1\} \subseteq T$?
(6) $\{1\} \subseteq S$?
(7) $T \subset R$?
(8) $\{1\} \in S$?
(9) $\emptyset \subseteq S$?
(10) $T \subseteq U$?
(11) $T \in U$?
(12) $T \notin R$?
(13) $T \subseteq R$?
(14) $S \subseteq \{1, 3, 9, 10\}$?

1.2.4. The powerset of a set. The powerset $\wp(S)$ of a set S is the set of all subsets of S.

EXEMPLE. What are the elements of the following powersets ?

(1) $\wp(\{1,2\}) =$
(2) $\wp(\{1\}) =$
(3) $\wp(\emptyset) =$

EXERCICE 2. What is the size of $\wp(S)$ if S has n elements ?

1.2.5. Binary and unary operations.

DÉFINITION. $\bullet$ is a *unary operation* on a set S if for every element x of S, $\bullet x$ exists, is unique and is a member of S.

$\bullet$ is a *binary operation* on a set S if for every ordered pair (x, y) of elements of S, $x \bullet y$ exists, is unique and is a member of S.

Examples:

(1) is $+$a binary operation on $\mathbb{N}$?
(2) is $+$a binary operation on $\{0, 1, 2\}$?
(3) is $\times$a binary operation on $\{0, 1\}$
(4) is $-$a binary operation on $\mathbb{N}$?
(5) is $/$a binary operation on $\mathbb{Z}$?
(6) are $+$,$-$, and $\times$binary operations on $\mathbb{Q}$?
(7) are $+$,$-$, $\times$and $/$binary operations on $\mathbb{Q}^*$?
(8) is $\sqrt{x}$ a unary operation on $\mathbb{R}^+$?
(9) are $\wedge$, $\vee$, $\rightarrow$, $'$, ... operations on $\{true, false\}$? on wff ?

A binary operation can be defined by its *multiplication* table.

EXEMPLE. $(\{true, false\}, \wedge)$

$\wedge$	$false$	$true$
$false$	$false$	$false$
$true$	$false$	$true$

An operation does not necessarily need to have a particular meaning.

EXEMPLE. $(\{2, 5, 9\}, \bullet)$

$\bullet$	2	5	9
2	2	5	2
5	2	9	5
9	9	2	5

$5 \bullet 9 =?$

1.3. Operations on sets

1.3.1. The universe of discourse. We have seen operations on numbers, or other objects.

We can also define operations on sets (union, intersection, ...).

We need a set that contains all the sets we want to deal with.

It would be tempting to consider the set of all sets.

PROBLEM 1.3.1. Let S be the set of all sets that does not contain themselves. Does S contain itself ?

- if S does not contain itself, then it contains itself !
- if S contains itself, then it does not contain itself !

There is a strange loop here which yields a contradiction: S cannot exist.

For a similar reason, *the set of all sets cannot exist.*

See *Gödel Esher Bach*[**?**] for a lot of similar fun stuff with strange loops.

That's been a major source of trouble and work a century ago, when mathematicians tried to define a strong basis for set theory.

To be safe, we always work inside a set big enough to contain all the sets we need, but small enough to avoid the strange loop above.

DÉFINITION. This set is the *universal set*, or the *universe of discourse.*

We define operations on the powerset of the universal set.

1.3.2. Union, intersection, complement and Cartesian product. We define operations on subsets of the universe of discourse.

DÉFINITION. The *union* of A and B is the set:

$$A \cup B := \{x \,|\, x \in A \text{ or } x \in B\}$$

DÉFINITION. The *intersection* of A and B is the set:

$$A \cap B := \{x \,|\, x \in A \text{ and } x \in B\}$$

DÉFINITION. The *complement* of A is the set:

$$A' := \{x \,|\, x \notin A\}$$

DÉFINITION. The *set difference* of A and B is the set:

$$A - B := \{x \,(x \in A) \text{ and } (x \notin B)\}$$

DÉFINITION. The *Cartesian product* (or *cross product*) of A and B is the set:

$$A \times B := \{(x, y) \,|\, x \in A, y \in B\}$$

NOTATION 1.3.2. $A^2 = A \times A$ is the set of all ordered pairs of elements of A; $A^n = A \times \cdots \times A$ is the set of all n-uples of elements of A.

DÉFINITION. *Venn diagrams.*

EXERCICE 3. *Let* $A := \{1, 2\}$ *and* $B := \{2, 3, 4\}$.

(1) $A \cup B =$,
(2) $A \cap B =$,
(3) $A - B =$,
(4) $A' =$ (assuming that the universe of discourse is $\{1, 2, 3, 4\}$),
(5) $A \times B =$,
(6) $A^3 =$.

EXERCICE 4. Let A be a set of size n, and B a set of size m.

(1) what is the size of $A \cup B$:
(2) what is the size of $A \cap B$:
(3) what is the size of A' ?
(4) what is the size of $A \times B$:

1.3.3. Set identities.

PROPOSITION. *Let A and B be to sets. Then,*
$A \cap B = B \cap A$ *(commutative property)*

PROOF. $x \in A \cap B$
$\Leftrightarrow (x \in A) \wedge (x \in B)$ by definition of $\cap$
$\Leftrightarrow (x \in B) \wedge (x \in A)$ by commutativity of $\wedge$
$\Leftrightarrow x \in B \cap A$ by definition of $\cap$ □

The commutativity of $\cap$derives directly from the commutativity of $\wedge$.
All identities on logic operators induce identities on set operators.

PROPOSITION. *Let A, B, and C be two sets. Then,*
$A \cup B = B \cup A$ *(commutative property)*
$A \cap B = B \cap A$ *(commutative property)*
$(A \cup B) \cup C = A \cup (B \cup C) = A \cup B \cup C$ *(associative property)*
$(A \cap B) \cap C = A \cap (B \cap C) = A \cap B \cap C$ *(associative property)*
$A \cup A' = S$ *(complement, S is the universe of discourse)*
$A \cap A' = \emptyset$ *(complement)*
$(A \cup B)' = A' \cap B'$ *(de Morgan's)*
$(A \cap B)' = A' \cup B'$ *(de Morgan's)*
$A - B = A \cap B'$

1.4. Countable and uncountable sets

1.4.1. Enumerations. If a set S has k elements, these can be listed one after the other:

$$s_1, s_2, \ldots, s_k$$

DÉFINITION. $s_1, s_2, \ldots, s_k$ is called an *enumeration* of the set S.

EXEMPLE. $1, 5, 4, 3$, $5, 1, 3, 4$, and $4, 1, 3, 5$ are enumerations of the set $\{1, 5, 4, 3\}$.

When a set S is infinite, you can not enumerate all of it's elements at once. However, some times, you can still pickup a first element s_1, then a second s_2, and so on forever. This process is an enumeration of the elements of S if:

- Any element of S gets enumerated eventually;
- No element is enumerated twice.

Exemple. $0, 1, 2, 3, 4, \ldots$ is an enumeration of the non-negative integers.

1.4.2. Denumerable and Countable sets.

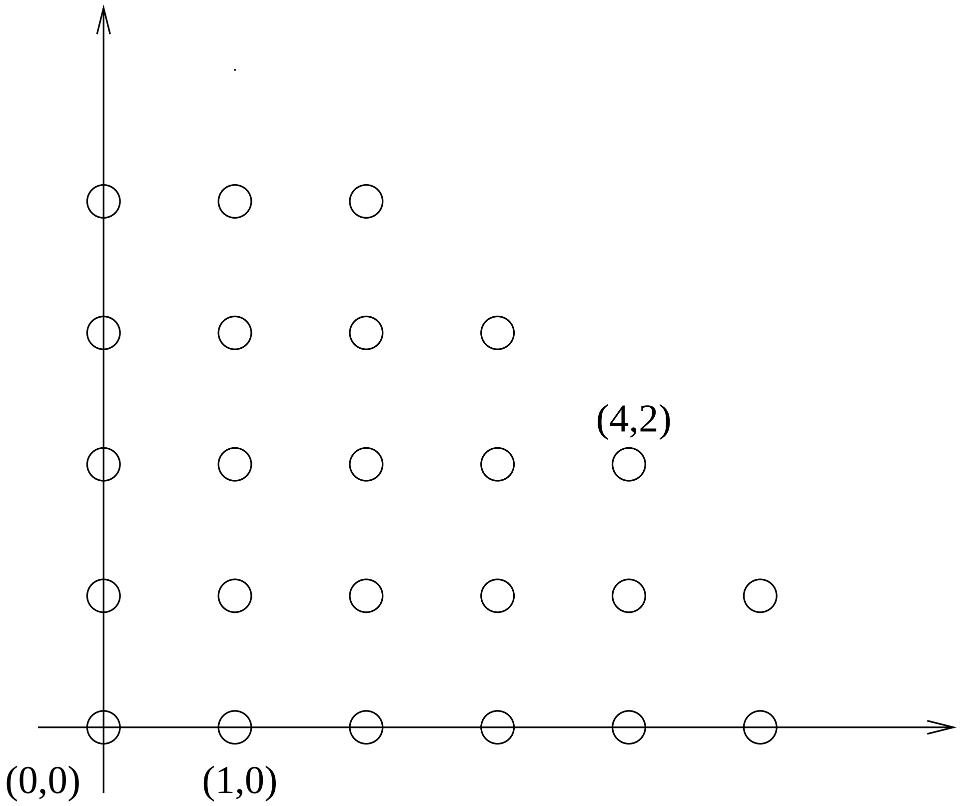
Définition. A infinite set S is *denumerable* if it has an enumeration

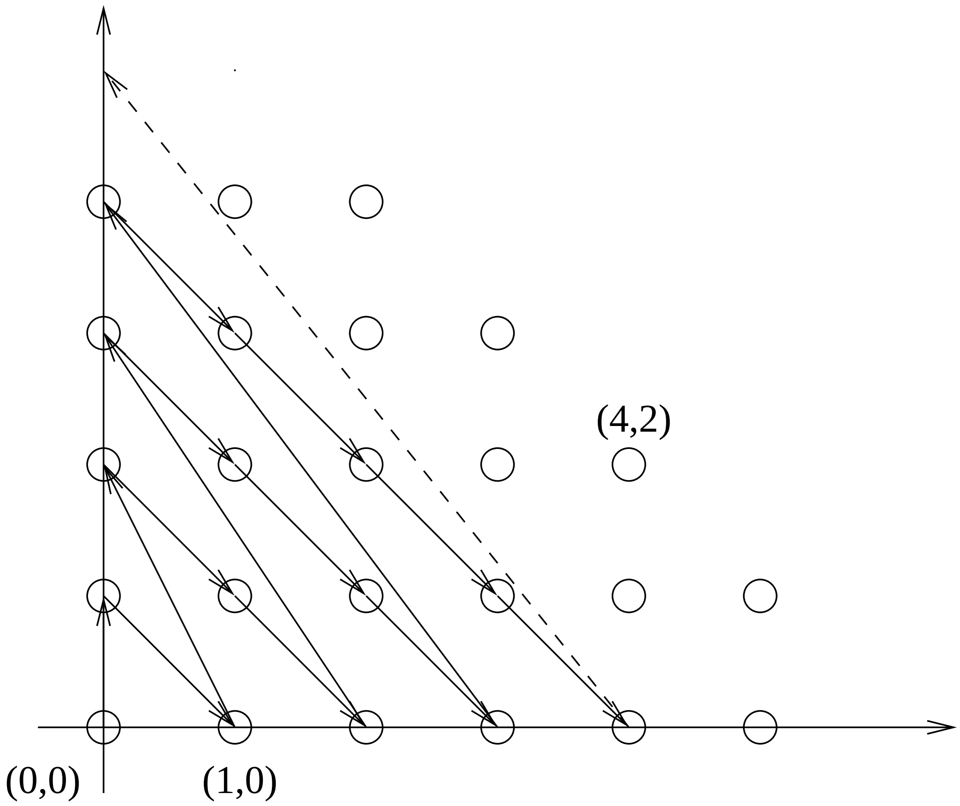
$$s_1, s_2, \ldots, s_n, \ldots$$

A set S is *countable* if it's either finite or denumerable.

Exemple. Are the following sets countable ?

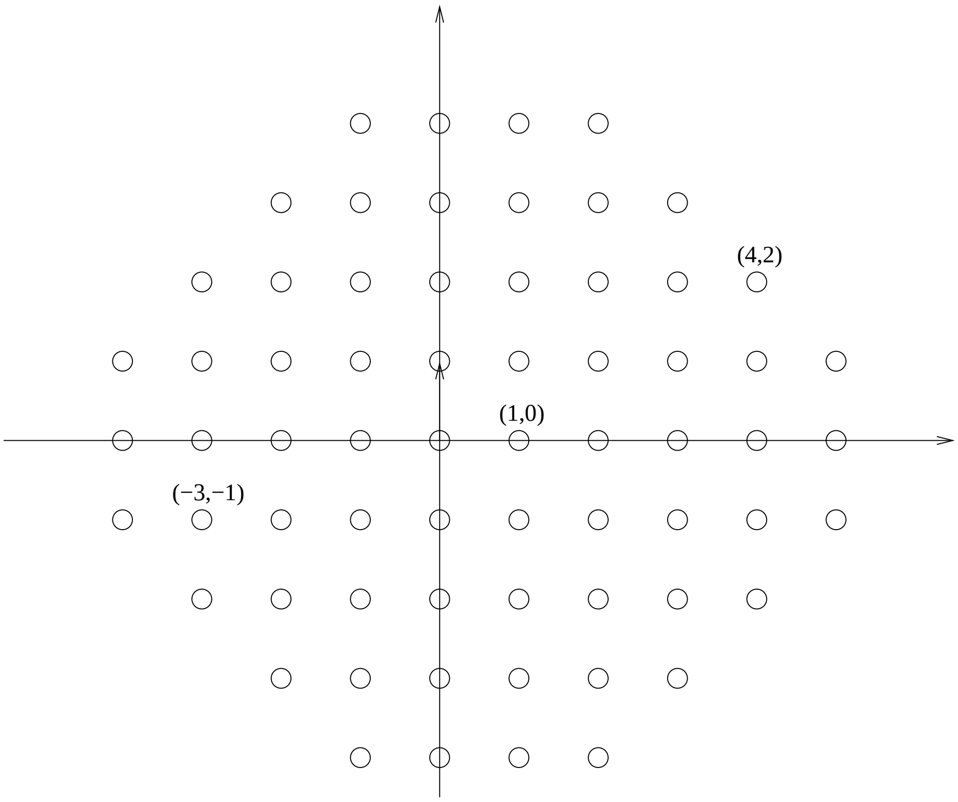
(1) The set of all students in this class.
(2) The set $\mathbb{N}$ of the non-negative integers (enumeration: $0, 1, 2, 3, 4, \ldots$);
Actually, the order does not need to be logical.
This is a perfectly legal enumeration: $0, 10, 5, 11, 4, 2, 17, 2, 1, 28, 3$
(3) The set of the even integers (enumeration: ;
(4) The set of the prime integers (enumeration: ;
(5) The set $\mathbb{Z}$ of the integers (enumeration:);
(6) The set $\mathbb{N} \times \mathbb{N}$
(e.g. all points in the plane with non-negative integer coordinates):

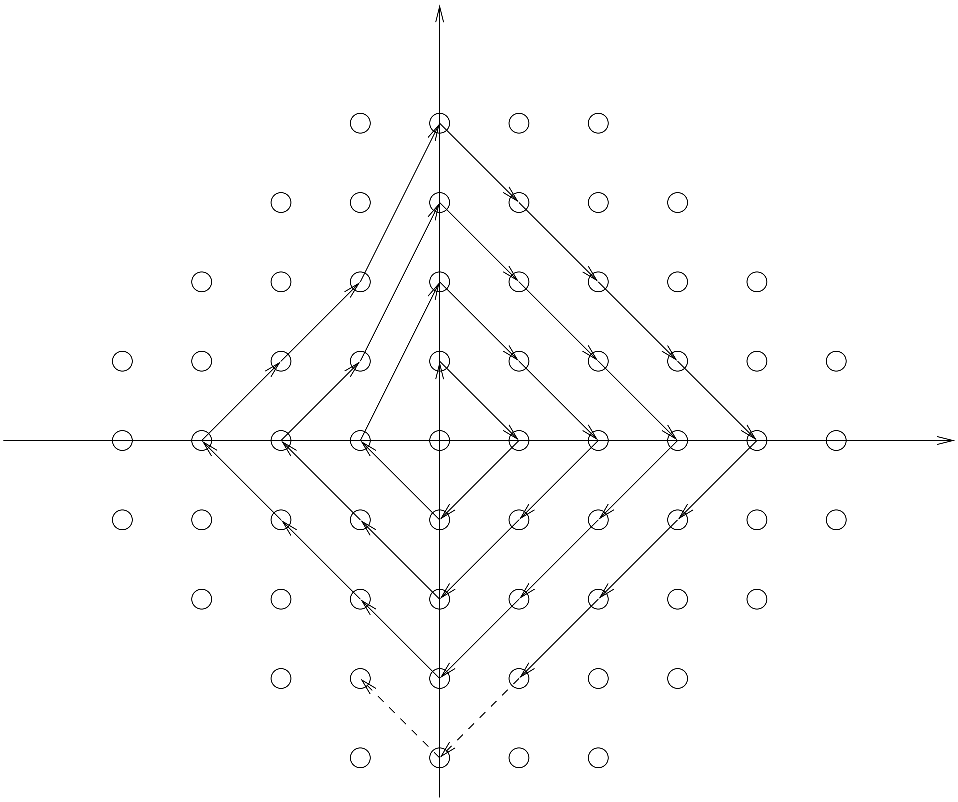




(7) Enumeration: $(0,0),(0,1),(1,0),(2,0),(1,1),(0,2),(3,0),\ldots$

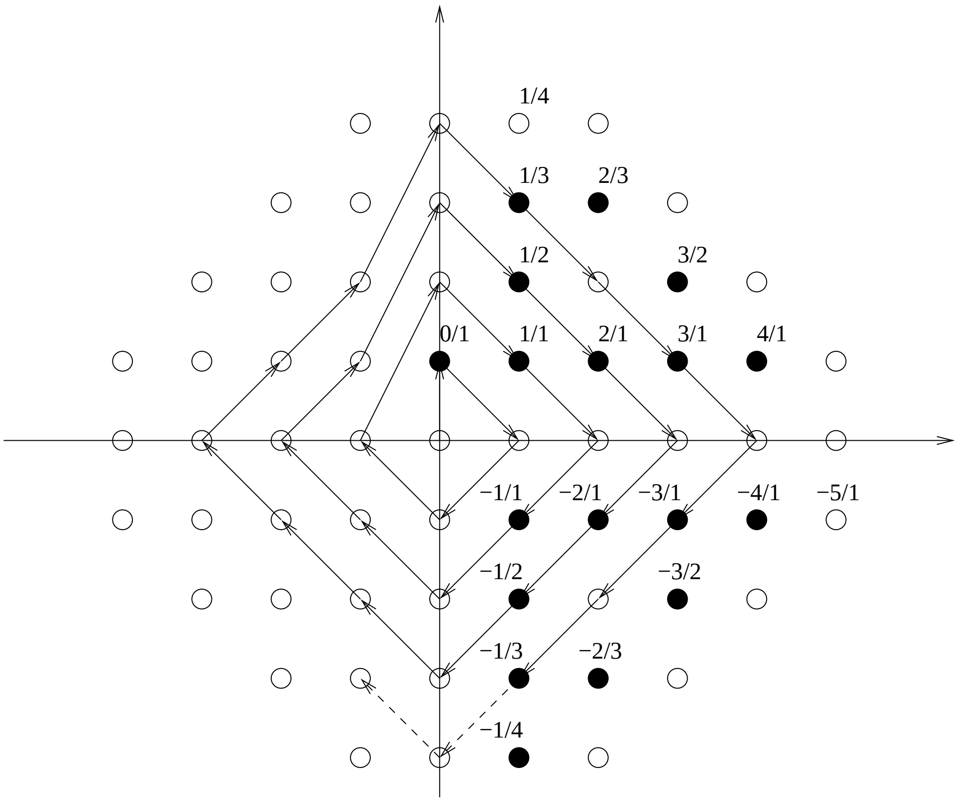
(8) The set $\mathbb{Z}\times\mathbb{Z}$ of all points in the plane with integer coordinates:


(4,2)
(1,0)
(−3,−1)



Enumeration: $(0,0),(0,1),(1,0),(0,-1),(-1,0),(2,0),\ldots$

(9) The set $\mathbb{Q}$ of rational numbers:



Théorème. *The following sets are countable:*

(1) *Any subset $A \subset B$ of a countable set B.*
(2) *The union $A \cup B$ of two countable sets A and B is countable.*
(3) *The union $A_1 \cup A_2 \cup \cdots \cup A_i$ of a finite number i of countable sets $A_1, \ldots, A_i$.*
(4) *The union $A_1 \cup A_2 \cup \cdots \cup A_i \cup \cdots$ of a countable number of countable sets.*
(5) *The cross product $A \times B$ of two countable sets A and B is countable.*
(6) *The cross product $A_1 \times \cdots \times A_i$ of a finite number of countable sets $A_1, \ldots, A_i$.*

Proof. Enumerations of those sets can be constructed in the following way: □

(1) Enumerate the elements of B, and ignore those that are not in A.
(2) Enumerate the elements of A and B alternatively $(a_1, b_1, a_2, b_2, \ldots)$.
(3) Induction, using 2.
(4) As for $\mathbb{N} \times \mathbb{N}$: $a_{1,1}, a_{2,1}, a_{1,2}, a_{3,1}, a_{2,2}, a_{1,3}, \ldots$ ($a_{i,j}$ is the jth element of A_i).
(5) As for $\mathbb{N} \times \mathbb{N}$: $(a_1, b_1), (a_1, b_2), (a_2, b_1), (a_1, b_3), (a_2, b_2), (a_3, b_1), \ldots$.
(6) Induction, using 5.

1.4.3. Uncountable sets ?

Remarque. All the sets we have seen so far are countable.

PROBLEM 1.4.1. Are there any uncountable sets ?

THÉORÈME. *(Cantor)* $\mathbb{R}$ *is uncountable.*

LEMME. *Any real number* $x \in [0,1)$ *can be written uniquely in decimal form:*

$$x = 0.d_1d_2d_3d_4 \cdots d_i \cdots ,$$

where the d_i *are digits between* 0 *and* 9*, and the sequence does not end by an infinite number of* 9.

EXEMPLE. Here is how some classical numbers can be written:

- $0 = 0.0000\cdots$
- $0.5 = 0.50000\cdots$
- $0.5 = 0.49999\cdots$ (Same number as above, we don't use this form)
- $\frac{1}{3} = 0.333333\cdots$
- $\pi = 3.141592653\cdots$

Let's jump to the proof of the theorem, without detailing the proof of this lemma.

PROOF. (Of the theorem): *Cantor diagonalization method.*
It's sufficient to prove that $[0,1)$ is not countable.
Let's do this by contradiction: assume $[0,1)$ is countable.
Let $s_1, s_2, \ldots, s_i, \ldots$ be an enumeration of $[0,1)$.
Goal: construct an element which is not in this enumeration.
Using the lemma, we can write the s_i as follow:

$$\begin{array}{ccccccccc}
s_1 & = & 0, & \underline{d_{1,1}} & d_{1,2} & d_{1,3} & d_{1,4} & d_{1,5} & \cdots \\
s_2 & = & 0, & d_{2,1} & \underline{d_{2,2}} & d_{2,3} & d_{2,4} & d_{2,5} & \cdots \\
s_3 & = & 0, & d_{3,1} & d_{3,2} & \underline{d_{3,3}} & d_{3,4} & d_{3,5} & \cdots \\
s_4 & = & 0, & d_{4,1} & d_{4,2} & d_{4,3} & \underline{d_{4,4}} & d_{4,5} & \cdots \\
s_5 & = & 0, & d_{5,1} & d_{5,2} & d_{5,3} & d_{5,4} & \underline{d_{5,5}} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

We want to construct an element x which is not in this enumeration.
Let's look at an example:

$$\begin{array}{cccccccc}
s_1 & = & 0, & \underline{1} & 5 & 7 & 3 & 5\cdots \\
s_2 & = & 0, & 0 & \underline{0} & 4 & 7 & 3\cdots \\
s_3 & = & 0, & 4 & 5 & \underline{7} & 0 & 3\cdots \\
s_4 & = & 0, & 9 & 7 & 3 & \underline{5} & 7\cdots \\
s_5 & = & 0, & 4 & 3 & 8 & 1 & \underline{0}\cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\ddots \\
 & & & & & & & \\
x & = & 0, & 0 & 1 & 0 & 0 & 1\cdots
\end{array}$$

The trick : let $x_i = 1$ if $d_{i,i} = 0$ and $x_i = 1$ else.
Then, $x \neq s_1$. But also, $x \neq s_2$, $x \neq s_3$, ...
Therefore x is indeed never enumerated! Contradiction!
Conclusion: $[0,1)$ is not countable. $\square$

REMARQUE. We can deduce that many sets like $\mathbb{C}$, or $[5.3, 10)$ are uncountable. A similar proof can be used to prove that many other sets are uncountable. This includes the set of all infinite strings, or the set $\wp(\mathbb{N})$ of all subsets of $\mathbb{N}$.

RÉSUMÉ 1.4.2. We have a hierarchy of bigger and bigger sets:

(1) The empty set
(2) Finite sets (the empty set, sets with 1 element, sets with 2 elements, ...)
(3) Denumerable sets: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, ...
(4) Uncountable sets: $\mathbb{R}$, $\mathbb{C}$, ...
(5) ...

PROBLEM 1.4.3. Is there any set bigger than $\mathbb{N}$ and smaller that $\mathbb{R}$? Nobody knows!

1.5. Conclusion

We are now done with basic properties of sets. We have seen enough formalism to go on to the next section, *Combinatorics*:

How to count the objects in a finite set ?