University of Toronto – MAT246H1-S – LEC0201/9201 – Winter 2021

Concepts in Abstract Mathematics

0 - Logic and sets

Jean-Baptiste Campesato

Contents

1 Sets

As in many areas of mathematics, we will use *sets* very often during this course. But we won't cover anything about axiomatic set theory. Instead we will only use a naive informal intuitive definition of what is a set and what is a function/map between two sets (you are already used to that from your linear algebra and calculus courses).

Definition 1 (Informal)**.** A *set* is a (well-defined) "collection" of elements (order doesn't matter).
Two sets are equal if they contain the same elements, so $\{1,2,2,3\} = \{1,2,3\}$ since they contain $1, 2, 3$.

Remark 2. We usually define a set either by giving explicitely the elements it contains, e.g.

$$S = \left\{\text{apple}, \pi, 5\right\}$$

or from an already constructed set by taking only the elements satisfying some property

$$S = \{n \in \mathbb{Z} \ : \ \exists k \in \mathbb{Z},\, n = 2k\}$$

Notation 3. Given a set S, we write $a \in S$ to express that a is an element of S. It is read *"a is in S"* or *"a is an element of S"*.

Example 4.
- $\text{apple} \in \left\{\text{apple}, \pi, 5\right\}$
- $\text{banana} \notin \left\{\text{apple}, \pi, 5\right\}$

Notation 5. Given two sets S and T, we write $S \subset T$ to express that every element of S is an element of T, i.e.

$$\forall a \in S,\, a \in T$$

It is read *"S is a subset of T"* or *"S is included in T"*.

Remark 6. Two sets S and T are equal if and only if they have the same elements, i.e.

$$S = T \Leftrightarrow \left(S \subset T \text{ and } T \subset S\right)$$

Remark 7. There exists a unique set containing no element, it is denoted by $\varnothing$ and called the *empty set*.

Remark 8. Given a set E, the set of subsets of E is well-defined, it is denoted by $\mathcal{P}(E) \coloneqq \{S \ : \ S \subset E\}$ and called the *powerset* of E.

2 Cartesian product

Definition 9. An *n-tuple* is an ordered list of n elements $(x_1, \dots, x_n)$. We say *couple* for a 2-tuple and *triple* for a 3-tuple.

Fundamental property 10. $(x_1, \dots, x_n) = (y_1, \dots, y_n) \Leftrightarrow x_1 = y_1,\ x_2 = y_2, \dots, x_n = y_n$

Remark 11.
- $\{1, 2, 3\} = \{3, 2, 1\}$ (*sets*)
- $(1, 2, 3) \neq (3, 2, 1)$ (*tuples*)

Remark 12.
- $\{1, 2, 2, 3\} = \{1, 2, 3\}$ (*sets*)
- $(1, 2, 2, 3) \neq (1, 2, 3)$ (*tuples*)

Theorem 13. *Given two sets A and B, the following set is well-defined*

$$A \times B \coloneqq \{(a, b)\ :\ a \in A,\ b \in B\}$$

It is called the cartesian product *of A and B.*

Example 14. Set $A = \{\pi, e\}$ and $B = \left\{1, \sqrt{2}, \pi\right\}$ then

$$A \times B = \left\{(\pi, 1), \left(\pi, \sqrt{2}\right), (\pi, \pi), (e, 1), \left(e, \sqrt{2}\right), (e, \pi)\right\}$$

Theorem 15. *Given sets $A_1, A_2, \dots, A_n$, the following set is well-defined*

$$A_1 \times A_2 \times \cdots \times A_n \coloneqq \{(a_1, a_2, \dots, a_n)\ :\ a_i \in A_i\}$$

Remark 16. We will often identify the following sets although they are not formally equal:
- $(A \times B) \times C \ni ((a, b), c)$
- $A \times (B \times C) \ni (a, (b, c))$
- $A \times B \times C \ni (a, b, c)$

3 Basic logic

Definition 17. A *statement* is a *sentence* which is either “true” (T) or “false” (F).

Definition 18. The *negation* of a statement P is the statement denoted by $\neg P$ (or no P) defined with the following truth table:

P	$\neg P$
V	F
F	V

Definition 19. The *disjunction* of two statements P and Q is the statement denoted by $P \vee Q$ (or P or Q) defined with the following truth table:

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

Beware: the disjunction is not exclusive.

Definition 20. The *conjunction* of two statements P and Q is the statement denoted by $P \wedge Q$ (or P and Q) defined with the following truth table:

P	Q	$P \wedge Q$
V	V	V
V	F	F
F	V	F
F	F	F

Definition 21. Given two statements P and Q, we define the statement $P \Rightarrow Q$ with the following truth table:

P	Q	$P \Rightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

It is called the *implication* (or *conditional statement*) and it is read as follows "P imples Q" or "if P (is true) then Q (is true)".

Definition 22. The *converse* of $P \Rightarrow Q$ is defined as $Q \Rightarrow P$.

Definition 23. Given two statements P and Q, we define the statement $P \Leftrightarrow Q$ with the following truth table:

P	Q	$P \Leftrightarrow Q$
V	V	V
V	F	F
F	V	F
F	F	V

It is called the *equivalence* and it is read "P is equivalent to Q" or "P (is true) if and only if Q (is true)".

Definition 24. A *tautology* is a statement which is true whatever are the truth values of its components, we usually use the notation $\models P$.

Definition 25. We say that P and Q are *logically equivalent* when $P \Leftrightarrow Q$ is a tautology.
It simply means that P and Q have the same truth table.

Remark 26. The above logical connectives could have been defined in terms of the disjunction and the negation. Indeed:

- $P \wedge Q$ is equivalent to $\neg((\neg P) \vee (\neg Q))$.

P	Q	$\neg P$	$\neg Q$	$(\neg P) \vee (\neg Q)$	$\neg((\neg P) \vee (\neg Q))$	$P \wedge Q$
V	V	F	F	F	V	V
V	F	F	V	V	F	F
F	V	V	F	V	F	F
F	F	V	V	V	F	F

- $P \Rightarrow Q$ is equivalent to $(\neg P) \vee Q$.

P	Q	$\neg P$	$(\neg P) \vee Q$	$P \Rightarrow Q$
V	V	F	V	V
V	F	F	F	F
F	V	V	V	V
F	F	V	V	V

- $P \Leftrightarrow Q$ is equivalent to $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ or to $(P \wedge Q) \vee ((\neg P) \wedge (\neg Q))$.

Example 27. *Law of excluded middle*: $\vDash P \vee (\neg P)$

P	$\neg P$	$P \vee (\neg P)$
V	F	V
F	V	V

The law of excluded middle simply means that either P is true, or its negation $\neg P$ is true.

Example 28. The *modus ponens*: $\vDash (P \wedge (P \Rightarrow Q)) \Rightarrow Q$

P	Q	$P \Rightarrow Q$	$P \wedge (P \Rightarrow Q)$	$(P \wedge (P \Rightarrow Q)) \Rightarrow Q$
V	V	V	V	V
V	F	F	F	V
F	V	V	F	V
F	F	V	F	V

It is the main inference rule in mathematics: if both P and $P \Rightarrow Q$ are true then so is Q.

Example 29. $\vDash (P \wedge Q) \Rightarrow P$

Example 30. $\vDash P \Rightarrow (P \vee Q)$

Proposition 31. *The disjunction is commutative:* $\vDash (P \vee Q) \Leftrightarrow (Q \vee P)$

Proposition 32. *The disjunction is associative:* $\vDash ((P \vee Q) \vee R) \Leftrightarrow (P \vee (Q \vee R))$*.*

Proposition 33. *The conjunction is commutative:* $\vDash (P \wedge Q) \Leftrightarrow (Q \wedge P)$

Proposition 34. *The conjunction is associative :* $\vDash ((P \wedge Q) \wedge R) \Leftrightarrow (P \wedge (Q \wedge R))$*.*

Proposition 35 (Double negation elimination)**.** $\vDash (\neg(\neg P)) \Leftrightarrow P$

Proof.

P	$\neg P$	$\neg(\neg P)$
V	F	V
F	V	F

■

Proposition 36 (Morgan's laws)**.**

- *The negation of* $P \vee Q$ *is* $(\neg P) \wedge (\neg Q)$*:*

$$\vDash (\neg(P \vee Q)) \Leftrightarrow ((\neg P) \wedge (\neg Q))$$

- *the negation of* $P \wedge Q$ *is* $(\neg P) \vee (\neg Q)$*:*

$$\vDash (\neg(P \wedge Q)) \Leftrightarrow ((\neg P) \vee (\neg Q))$$

Mnemonic device: the negation changes conjunctions in disjunctions and vice-versa.

Proof. I only prove the first one.

P	Q	$\neg P$	$\neg Q$	$(\neg P) \wedge (\neg Q)$	$P \vee Q$	$\neg(P \vee Q)$
V	V	F	F	F	V	F
V	F	F	V	F	V	F
F	V	V	F	F	V	F
F	F	V	V	V	F	V

■

Proposition 37 (Distributivity).
- $\vDash (P \wedge (Q \vee R)) \Leftrightarrow ((P \wedge Q) \vee (P \wedge R))$
- $\vDash (P \vee (Q \wedge R)) \Leftrightarrow ((P \vee Q) \wedge (P \vee R))$

Proposition 38 (Proof by contrapositive).
The statement $P \Rightarrow Q$ is logically equivalent to its contrapositive $(\neg Q) \Rightarrow (\neg P)$.

Proof.

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg Q$	$(\neg Q) \Rightarrow (\neg P)$
V	V	V	F	F	V
V	F	F	F	V	F
F	V	V	V	F	V
F	F	V	V	V	V

■

In some cases, it may be easier to prove $(\neg Q) \Rightarrow (\neg P)$ rather than $P \Rightarrow Q$.

Example 39. Let $n \in \mathbb{Z}$. Prove that if n^2 is odd then n is odd.

Proposition 40 (Reductio ad absurdum). $(((\neg P) \Rightarrow Q) \wedge ((\neg P) \Rightarrow (\neg Q))) \Rightarrow P$ *is a tautology.*

In practice, in order to prove P by contradiction, we assume that $\neg P$ is true and we look for a contradiction.

4 Quantifiers

Definition 41. A *predicate* $P(x, y, \dots)$ is a statement whose truth value depends on variables $x, y, \dots$ occuring in it.

Definition 42 (Universal quantifier). The statement "$\forall x \in E,\ P(x)$" means that $P(x)$ is true for any x in E.
It is read "for all x in E, $P(x)$ is true".

Definition 43 (Existential quantifier). The statement "$\exists x \in E,\ P(x)$" means that there exists at least one x in E such that $P(x)$ is true.
It is read "there exists x in E such that $P(x)$ is true".

Here x is a bound variable:
- we may replace "$\forall x \in E,\ P(x)$" by "$\forall y \in E,\ P(y)$"
- we may replace "$\exists x \in E,\ P(x)$" by "$\exists y \in E,\ P(y)$".

Definition 44. The statement "$\exists! x \in E,\ P(x)$" means that $P(x)$ is true for exactly one element x in E.
It is read "there exists a unique x in E such that $P(x)$ is true".

As we see in the following example, we can't permute the quantifiers $\forall$ and $\exists$.
- $\exists n \in \mathbb{N},\ \forall p \in \mathbb{N},\ p \leq n$
- $\forall p \in \mathbb{N},\ \exists n \in \mathbb{N},\ p \leq n$

Nonetheless, we may permute two existential quantifiers or two universal quantifiers.

Remark 45. It is common to write "$\forall x, y \in E$" for "$\forall x \in E,\ \forall y \in E$" (that's an ellipsis).
The same holds for the existential quantifier $\exists$.

Definition 46. The negation of "$\forall x \in E,\ P(x)$" is "$\exists x \in E,\ \neg P(x)$".

Definition 47. The negation of "$\exists x \in E,\ P(x)$" is "$\forall x \in E,\ \neg P(x)$".

Mnemonic device: the negation swaps $\forall$ and $\exists$.

Axiom 48. The statement "$\exists x \in \varnothing,\ P(x)$" is false for any predicate.

Proposition 49. *The statement "$\forall x \in \varnothing,\ P(x)$" is true for any predicate.*

Proof. Indeed, $\exists x \in \varnothing, (\neg P(x))$ is false, so its negation $\forall x \in \varnothing,\ P(x)$ is true. ■

5 Functions

Definition 50 (informal)**.** A *function* (or *map*) is the data of two sets A and B together with a "process" which assigns to each $x \in A$ a unique $f(x) \in B$:

$$f : \begin{cases} A & \to & B \\ x & \mapsto & f(x) \end{cases}$$

Here, f is the name of the function, A is the *domain* of f, and B is the *codomain* of f.

Remark 51. The domain and codomain are part of the definition of a function. For instance

$$f : \begin{cases} \mathbb{R} & \to & [1, +\infty) \\ x & \mapsto & x^2 + 1 \end{cases} \qquad \text{and} \qquad g : \begin{cases} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^2 + 1 \end{cases}$$

are not the same function (the first one is surjective but not the second one).
A function is not simply a "formula", you need to specify the domain and the codomain.

Definitions 52. Given a function $f : A \to B$.

- The *image of $E \subset A$ by f* is $f(E) \coloneqq \{f(x) : x \in E\} \subset B$.
- The *image of f* (or *range of f*) is $\mathrm{Range}(f) \coloneqq f(A)$.
- The *preimage of $F \subset B$ by f* is $f^{-1}(F) \coloneqq \{x \in A : f(x) \in F\}$.
- The *graph of f* is the set $\Gamma_f \coloneqq \{(x, y) \in A \times B : y = f(x)\}$.
- We say that f is *injective* (or *one-to-one*) if $\forall x_1, x_2 \in A,\ x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$ or equivalently by taking the contrapositive $\forall x_1, x_2 \in A,\ f(x_1) = f(x_2) \implies x_1 = x_2$
- We say that f is *surjective* (or *onto*) if $\forall y \in B,\ \exists x \in A,\ y = f(x)$
- We say that f is *bijective* if it is injective and surjective, i.e. $\forall y \in B,\ \exists! x \in A,\ y = f(x)$

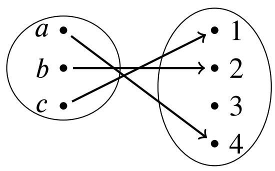

Figure 1: Injective

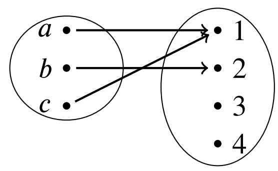

Figure 2: Not injective

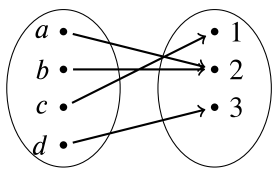

Figure 3: Surjective

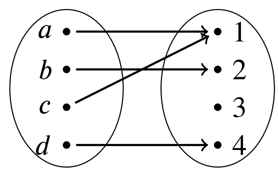

Figure 4: Not surjective

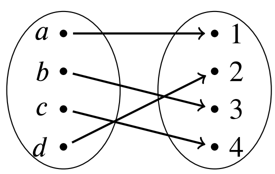

Figure 5: Bijective

Proposition 53. *$f : A \to B$ is bijective if and only if there exists $g : B \to A$ such that* $\begin{cases} \forall x \in A,\ g(f(x)) = x \\ \forall y \in B,\ f(g(y)) = y \end{cases}$.
Then g is unique, it is called the inverse of f *and denoted by* $f^{-1} : B \to A$.

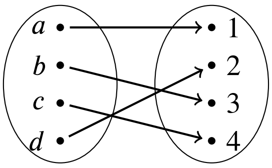

Figure 6: Bijective function

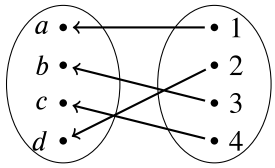

Figure 7: Its inverse

6 Sigma notation

Definition 54. For $m, n \in \mathbb{Z}$, we set

$$\sum_{i=m}^{n} a_i = a_m + a_{m+1} + \cdots + a_n$$

Remark 55. If $m > n$ then $\sum_{i=m}^{n} a_i = 0$ by convention.

Example 56. $\sum_{i=3}^{7} i^2 = 3^2 + 4^2 + 5^2 + 6^2 + 7^2 = 135$

Remark 57. If $m \leq n$ then there are $n - m + 1$ terms in the sum $\sum_{i=m}^{n} a_i$.