Math 300

Corse Notes

Contents

1 Sets and quantifiers

1.1 Introduction to set notation

Informal Definition. A *set* is a collection of objects.

Conventions.

- Sets are frequently denoted by uppercase letters (e.g. A, B, C).
- If x is in A, then we say that x is an *element* of A or that A *contains* x, and we write $x \in A$.
- Otherwise, we write $x \notin A$.
- If the elements of A are precisely $a_1, \ldots, a_n$, then we write $A = \{a_1, \ldots, a_n\}$.

Examples.

i. natural numbers $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$[1]

ii. integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

iii. rational numbers $\mathbb{Q}$

iv. real numbers $\mathbb{R}$

v. complex numbers $\mathbb{C}$

Convention. If the elements of A are precisely those of B that satisfy a condition P, then we write

$$A = \{x \in B \,|\, x \text{ satisfies the condition } P\}.$$

Examples.

i. $\mathbb{N} = \{n \in \mathbb{Z} \,|\, n \geq 0\}$

ii. $\mathbb{Q} = \left\{ \frac{n}{m} \,\middle|\, n, m \in \mathbb{Z}, m \neq 0 \right\}$

Definition. The *empty set* $\varnothing$ is the set that contains no elements.

That is, $\varnothing = \{\}$.

1.2 Quantifiers

Informal Definition. If there is an element $x \in A$ that satisfies the condition P, then we write

$$\exists\, x \in A : x \text{ satisfies the condition } P.$$

The symbol $\exists$ is called the *existential quantifier*.

Convention. There are a few ways this can be read. Examples include,

- "There exists an x in A such that x satisfies P."
- "There is an x in A such that…"
- "There is an x in A that satisfies the condition P."

Examples. The following statements are true:

i. $\exists\, n \in \mathbb{Z} : n$ is even

ii. $\exists\, x \in \mathbb{R} : x > 3$

iii. $\exists\, n \in \mathbb{N} : n > 3$ and n is even

[1] There is an alternative convention that $\mathbb{N} = \{1, 2, 3, \ldots\}$.

The following are false:

iv. $\exists\, n \in \mathbb{N} : n < 0$

v. $\exists\, n \in \mathbb{Z} : n > 3$ and $n < 1$

vi. $\exists\, x \in \mathbb{R} : x^2 = -1$

Informal Definition. If every $x \in A$ satisfies the condition P, then we write

$$\forall\, x \in A : x \text{ satisfies the condition } P.$$

The symbol $\forall$ is called the *universal quantifier*.

Convention. This may be read as, for example,

- "For all/every/any x in A, x satisfies the condition P"
- "All x in A satisfy…"
- "Every/Any x in A satisfies…"

Examples. True statements:

i. $\forall n \in \mathbb{N} : n \geq 0$

ii. $\forall k \in \mathbb{N} : k \in \mathbb{Z}$

iii. $\forall x \in \mathbb{R} : x^2 \geq 0$

False statements:

iv. $\forall x \in \mathbb{R} : x \in \mathbb{N}$

v. $\forall m \in \mathbb{Z} : m$ is even

vi. $\forall n \in \mathbb{N} : \sqrt{n} \in \mathbb{N}$

Remark. Note that

$$\text{If } x \in A, \text{ then } P(x)$$

may also be formalized as

$$\forall x \in A : P(x).$$

Examples. Quantifiers can be strung together:

i. $\forall m \in \mathbb{Z} : \exists n \in \mathbb{N} : m < n$

ii. $\forall x \in \mathbb{R} : \exists y \in \mathbb{R} : x - y = 2$

iii. $\forall x \in \mathbb{R} : \exists y \in \mathbb{R} : \forall z \in \mathbb{R} : (x - y)z = 0$

Convention. When introducing new variables of the same type, it is convenient to do so alphabetically (e.g. a, b, c, or x, y, z).

1.3 Proofs with quantifiers

To prove a claim of the form

$$\exists x \in A : P(x),$$

we have simply to exhibit an $x \in A$ that satisfies the condition P.

Consider the following example:

Claim. *There is a $k \in \mathbb{Z}$ such that $k^2 = k$.*

Proof. We have $0 \in \mathbb{Z}$ and $0^2 = 0$. □

Remark. We could have just as well chosen $k = 1$. Only a single $k \in \mathbb{Z}$ satisfying $k^2 = k$ is required to prove the claim.

Convention. A proof should consist of grammatically correct English sentences. It is considered undesirable to begin a sentence with a mathematical symbol. To adhere to this rule, it is often convenient to preface an otherwise-bare mathematical formula with a brief phrase such as

- "We have..."
- "Observe that..."
- "Note that..."

To prove a claim of the form

$$\forall x \in A : P(x),$$

there are two steps:

1. Introduce an arbitrary $x \in A$.
2. Show that x satisfies P.

The first step is accomplished by means of a statement such as

- "Let $x \in A$."
- "Fix $x \in A$."
- "Suppose that $x \in A$."

Claim. *If $q \in \mathbb{Q}$, then $\frac{q}{2} \in \mathbb{Q}$.*

Proof. Fix $q \in \mathbb{Q}$. By the definition of $\mathbb{Q}$, there are $m, n \in \mathbb{Z}$ with $n \neq 0$ such that $q = \frac{m}{n}$. Thus,

$$\frac{q}{2} = \frac{m}{2n} \in \mathbb{Q}.$$

□

Convention. Common prefaces to a conclusion include

- "Thus,"
- "Hence,"
- "Therefore,"
- "It follows that,"

Claim. *For every $m \in \mathbb{Z}$, there is an $n \in \mathbb{Z}$ with $m < n$.*

Proof. Fix $m \in \mathbb{Z}$ and let $n = m + 1$. It follows that $m < n$. $\square$

Convention. The following phrases have similar meanings:

- "such that"
- "with"
- "subject to the condition that"
- "satisfying"
- "for which"

2 Logical connectives

2.1 Negation

Informal Definition. The *negation* of a statement S is the statement that *it is not the case that* S, written $\neg S$.

Convention. The symbol $\neg$ is read "not".

Examples. i. The negation of

$$\exists\, x \in \mathbb{R} : x^2 = -1$$

is

$$\neg\exists\, x \in \mathbb{R} : x^2 = -1,$$

which states that *it is not the case that* there is a real number that squares to -1.

ii. The negation of

$$\forall n \in \mathbb{Z} : n \geq 0$$

is

$$\neg\forall n \in \mathbb{Z} : n \geq 0,$$

which asserts that *it is not the case that* every integer is positive.

Informal Definition. To *disprove* a statement S is to prove that S is false. This is equivalent to proving $\neg S$.

It is useful to note that

$$\neg\forall x \in A : P(x) \qquad \text{is equivalent to} \qquad \exists x \in A : \neg P(x)$$

and

$$\neg\exists x \in A : P(x) \qquad \text{is equivalent to} \qquad \forall x \in A : \neg P(x).$$

Examples. i. The negation of

$$\exists x \in \mathbb{R} : \forall y \in \mathbb{R} : x = y$$

is

$$\forall x \in \mathbb{R} : \exists y \in \mathbb{R} : x \neq y$$

ii. The negation of

$$\forall m \in \mathbb{Z} : \exists n \in \mathbb{N} : m + n < 0$$

is

$$\exists m \in \mathbb{Z} : \forall n \in \mathbb{N} : m + n \geq 0$$

Proof of i. Fix $x \in \mathbb{R}$. If $y = x + 1$, then $x \neq y$. □

Proof of ii. Put $m = 0$ and let $n \in \mathbb{N}$. Since $n \geq 0$, it follows that $m + n \geq 0$. □

2.2 Logical connectives

Informal Definition. We implement the following shorthand.

symbol	meaning
$\wedge$	and
$\vee$	or
$\to$, $\implies$	if ... then
$\leftrightarrow$, $\iff$	if and only if (precisely if, precisely when,...)

Examples. The following statements are true,

i. $(3 = 3) \wedge (5 = 5)$

ii. $(1 = 1) \vee (2 > 3)$

iii. $(5 < 6) \vee (5 < 7)$

iv. $\forall x \in \mathbb{R} : (x > 3) \to (x > 0)$

v. $(1 = 2) \to (7 \geq 5)$

vi. $\forall k \in \mathbb{N} : (k^2 = 4) \leftrightarrow (k = 2)$

and the following are false,

vii. $\forall x \in \mathbb{R} : (x^2 = 4) \leftrightarrow (x = 2)$

viii. $\forall k \in \mathbb{Z} : (k > 5) \to (k > 8)$

To prove a

- *conjunction* $P \wedge Q$, you must prove both P and Q.
- *disjunction* $P \vee Q$, suppose that P is *false* and prove Q.
- *implication* $P \to Q$, supoose that P is *true* and prove Q.

Remark. When proving an implication $P \to Q$, the assumption P is often left unstated.

Claim. *For every $x \in \mathbb{R}$ there is a $y \in \mathbb{R}$ such that $y < x$ and $y < 0$.*

Proof. Fix $x \in \mathbb{R}$ and let y be the minimum of $x - 1$ and -1. It follows that $y < x$ and $y < 0$. $\square$

Claim. *Let $x \in \mathbb{R}$. If $x^2 = x$, then $x = 0$ or $x = 1$.*

Proof. Suppose that $x^2 = x$ and $x \neq 0$. Dividing both sides of $x^2 = x$ by $x \neq 0$ yields $x = 1$. $\square$

Alternative proof. Suppose that $x^2 = x$ and $x \neq 1$. Dividing both sides of $x(x-1) = 0$ by $x - 1 \neq 0$ provides $x = 0$. $\square$

Claim. *Let $x \in \mathbb{R}$. If $xy = y$ for all $y \in \mathbb{R}$, then $x = 1$.*

Proof. From the condition that $xy = y$ for all $y \in \mathbb{R}$, we conclude that $x = x \cdot 1 = 1$. $\square$

Informal Definition. We write

$$\exists!\, x \in A : P(x)$$

when there exists a *unique* $x \in A$ that satisfies the property P.

This is equivalent to

$$\exists\, x \in A : P(x) \wedge \Big(\forall y \in A : P(y) \to x = y\Big).$$

Examples. We have

i. $\exists! x \in \mathbb{R} : x^3 = 8$

ii. $\forall x \in \mathbb{R} : \exists! k \in \mathbb{Z} : k \leq x < k+1$

Claim. *There is a unique $m \in \mathbb{N}$ satisfying the property that $m \leq n$ for all $n \in \mathbb{N}$.*

Proof. Put $m = 0$. For all $n \in \mathbb{N}$, we have $m \leq n$. Now suppose that $m' \in \mathbb{N}$ satisfies $m' \leq n$ for all $n \in \mathbb{N}$. In particular, $m' \leq 0$ and $0 \leq m'$. Thus, $m = 0$. □

Remark. The expression

$$\forall x \in A : P(x)$$

is shorthand for

$$\forall x : \big(x \in A \to P(x)\big)$$

3 Sets operations and functions

3.1 Assorted abbreviations

abbr.	Latin	meaning
e.g.	*exempli gratia*	for example
i.e.	*id est*	that is
viz.	*videlicet*	namely
cf.	*confer*	compare (*erroneously:* see)
ff.	*foliis*	following
ibid.	*ibidem*	in the same place (followed by page number)
op. cit.	*opere citato*	in the work cited (in the same work)
loc. cit.	*loco citato*	in the place cited (on the same page)
QED	*quod erat demonstrandum*	that which was to be shown

3.2 Union, intersection, containment, and complement

Let A and B be sets.

Definition. The *union* of A and B is

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

Example. If A and B are the sets of even and odd integers, respectively, then $A \cup B = \mathbb{Z}$.

Definition. The *intersection* of A and B is

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

Example. We have

$$\mathbb{N} = \mathbb{Z} \cap \mathbb{R}_{\geq 0}$$

where $R_{\geq 0} = \{x \in \mathbb{R} \,|\, x \geq 0\}$ is the set of nonnegative real numbers.

Definition. We say that A and B are *disjoint* when $A \cap B = \varnothing$.

Example. Every set A is disjoint from the empty set $\varnothing$.

Definition. We say that A is a *subset* of B if

$$\forall x : \big(x \in A \to x \in B\big).$$

In this case, we write $A \subseteq B$.

Examples. We have

i. $\varnothing \subseteq A$ for every set A,

ii. $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Definition. The *difference* of A and B is

$$B \backslash A = \{x \in B \,|\, x \notin A\}.$$

Example. The set of irrational numbers is $\mathbb{R} \backslash \mathbb{Q}$.

Definition. If $A \subseteq B$, then the *complement* of A in B is $A^c = B \backslash A$.

Example. The complement of the set of even integers is the set of odd integers.

Claim. *Let A, B, and C be sets. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.*

To prove this, we will assume that $A \subseteq B$ and $B \subseteq C$, and we must deduce that $A \subseteq C$.

Proof. Fix $x \in A$. From $A \subseteq B$ we obtain $x \in B$, and from $B \subseteq C$ we conclude that $x \in C$. □

3.3 First definitions and examples

Let A and B be sets.

Informal Definition. A *function* $f : A \to B$ is a rule that assigns to each $x \in A$ a unique $f(x) \in B$.

$$\forall x \in A : \exists! y \in B : y = f(x)$$

Remark. We sometimes write $x \mapsto f(x)$ to

Examples. i. Consider

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{N} \\ k &\mapsto 2k. \end{aligned}$$

ii. The *identity function* on A is

$$\begin{aligned} f : A &\to A \\ x &\mapsto x. \end{aligned}$$

iii. The *constant function* $f : A \to B$ with value $b \in B$ is

$$\begin{aligned} f : A &\to B \\ x &\mapsto b. \end{aligned}$$

iv. The *empty function* $f : \varnothing \to B$ is completely determined by the value it assigns each element in $\varnothing$.

v. If $A \subseteq B$ then the associated *inclusion function* is

$$\begin{aligned} f : A &\to B \\ x &\mapsto x. \end{aligned}$$

vi. We may consider a property $P(x)$ that elements $x \in A$ can satisfy as a function

$$\begin{aligned} P : A &\to \mathbb{B} \\ x &\mapsto P(x) \end{aligned}$$

where $\mathbb{B} = \{\top, \bot\}$ is the Boolean domain, comprising the *truth values* true $\top$ and false $\bot$.

Definition. The *composition* of $f : A \to B$ and $g : B \to C$ is

$$\begin{aligned} g \circ f : A &\to C \\ x &\mapsto g(f(x)). \end{aligned}$$

4 Injective and surjective functions

4.1 Shortening proofs

Claim. *Let $x \in \mathbb{R}$. If $x > 0$, then there is a $y \in \mathbb{R}$ such that $0 < y < x$.*

Formally, this is

$$\forall x \in \mathbb{R} : \exists y \in \mathbb{R} : 0 < y < x$$

Proof. Fix $x \in \mathbb{R}$. Suppose that $x > 0$. Put $y = \frac{x}{2}$ and observe that $0 < y < x$. $\square$

Informal Definition. We will say that a *fully explicit proof* is a proof that explicitly

i. states every assumption and introduces every variable,

ii. validates every statement.

Actual proofs in the mathematical literature are hardly ever fully explicit. In particular, actual proofs will often refrain from

i. stating every assumption or introducing every variable. This is particularly common when the assumptions would be stated at the opening of a proof.

   Proof. Put $y = \frac{x}{2}$ and observe that $0 < y < x$. $\square$

ii. validates every statement. When a statement is obvious, it is often omitted.

   Proof. Fix $x \in \mathbb{R}$. Suppose that $x > 0$ and put $y = \frac{x}{2}$. $\square$

Taken together, we have

Proof. Put $y = \frac{x}{2}$. $\square$

The balance between what to make explicit and what to keep implicit in a proof depends on the intended audience. A guiding principle is that

Given your proof, the intended reader should be able to easily write a fully explicit proof.

Remark. In general, when a statement is obvious, it does not need to be proved. Be aware that the word *obvious* (or its synonyms *clear*, *apparent*, *trivial*, *elementary*,...) mean "obvious how to prove" and not "obvious that it is true".

4.2 Injectivity and surjectivity

Definition. The function $f : A \to B$ is said to be *injective* if $f(x) = f(y)$ implies $x = y$.

$$\forall x, y \in A : \big(f(x) = f(y)\big) \implies (x = y)$$

Claim. *The function $f : \mathbb{N} \to \mathbb{N}$ given by $f(k) = 2k$ is injective.*

Proof. Let $k, \ell \in \mathbb{N}$ and suppose that $f(k) = f(\ell)$. Dividing both sides of $2k = 2\ell$ by 2 yields $k = \ell$. $\square$

Claim. *The constant function $f : \mathbb{R} \to \mathbb{Z}$ with value 0 is not injective.*

We must show that

$$\exists x, y \in \mathbb{R} : \big(f(x) = f(y)\big) \wedge (x \neq y).$$

Proof. We have $f(1) = 0 = f(2)$ but $1 \neq 2$. $\square$

Definition. The function $f : A \to B$ is called *surjective* when for every $y \in B$ there is an $x \in A$ with $f(x) = y$.

$$\forall y \in B : \exists x \in A : f(x) = y$$

Claim. *The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is not surjective.*

We must show that

$$\exists y \in \mathbb{R} : \forall x \in \mathbb{R} : f(x) \neq y$$

Proof. From $x^2 \geq 0$ for all $x \in \mathbb{R}$, it follows that $f(x) \neq -1$ for any $x \in \mathbb{R}$. $\square$

Definition. We say that $f : A \to B$ is *bijective* when it is both injective and surjective.

Claim. *The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 2x$ is bijective.*

Proof. If $x, y \in \mathbb{R}$ satisfy $2x = 2y$, then division by 2 yields $x = y$. This proves injectivity.

To establish surjectivity, fix $y \in \mathbb{R}$ and observe that $2(\frac{y}{2}) = y$. $\square$

4.3 More proofs with functions

Let A, B, and C be sets and let $S \subseteq A$ be a subset.

Claim. *If $f : A \to B$ and $g : B \to C$ are injective, then $g \circ f : A \to C$ is injective.*

We must show that

$$\forall x, y \in A : g \circ f(x) = g \circ f(y) \implies x = y$$

Proof. Suppose that $g\big(f(x)\big) = g\big(f(y)\big)$. From the injectivity of g we have $f(x) = f(y)$, and from the injectivity of f we conclude that $x = y$. $\square$

Claim. *If $f : A \to B$ and $g : B \to C$ are surjective, then $g \circ f : A \to C$ is surjective.*

Now we must show that

$$\forall c \in C : \exists a \in A : g \circ f(a) = c$$

Proof. From the surjectivity of g there is a $b \in B$ such that $g(b) = c$, and from the surjectivity of f there is an $a \in A$ with $f(a) = b$. Thus, $g(f(a)) = g(b) = c$. $\square$

Claim. *If $f : A \to B$ and $g : B \to A$ satisfy $g \circ f = \mathrm{id}_A$, then f is injective and g is surjective.*

Proof. Suppose that $f(a) = f(a')$. Applying g to each side, we obtain $a = g(f(a)) = g(f(a')) = a'$. This establishes the injectivity of f.

Now fix $a \in A$ and observe that $g(f(a)) = a$. This proves the surjectivity of g. $\square$

Definition. The *restriction* of $f : A \to B$ to S is the function

$$\begin{aligned} f|_S : S \to \ & B \\ x \mapsto \ & f(x). \end{aligned}$$

Claim. *If $f : A \to B$ is injective, then $f|_S : S \to B$ is injective.*

Proof. Let $x, y \in S$ with $f(x) = f(y)$. By the injectivity of f, we have $x = y$. $\square$

Claim. *If $f : A \to B$ is surjective, then it is not necessarily true that $f|_S : S \to B$ is surjective.*

Proof. Suppose that B is nonempty, put $S = \varnothing \subseteq A$, and observe that $f|_S : S \to B$ is not surjective. $\square$