Lecture 1a

The natural numbers and induction

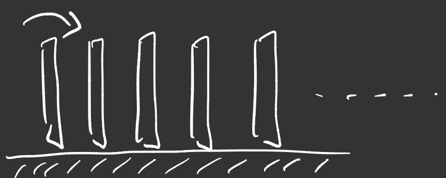
Definition A natural number is a member of the sequence $0, 1, 2, \dots$ formed by starting from 0 and successively adding 1. We write $\mathbb{N} = \{0, 1, 2, \dots\}$.

Remark 0 is sometimes included in $\mathbb{N}$, and sometimes not.

- We can add and multiply natural numbers. So if $m, n \in \mathbb{N}$ then $m + n$ and $m \times n$ are also natural numbers. ($m \times n$ is often written mn)
- Two important natural numbers are 0 and 1, which are the additive and multiplicative identities, i.e. for any $n \in \mathbb{N}$, $n + 0 = n$ and $n \times 1 = n$.
- The natural numbers have an ordering, so we can write things like $m \leq n$.

Definition Let $m, n \in \mathbb{N}$. We write $m \leq n$ to mean that there exists a natural number k such that $m + k = n$.

'Theorem' (Principle of mathematical induction). Let $P(n)$ be a family of statements indexed by the natural numbers. Suppose (i) $P(0)$ is true, and (ii) for any $n \in \mathbb{N}$, if $P(n)$ is true then $P(n+1)$ is true. Then $P(n)$ is true for all $n \in \mathbb{N}$.



Proposition For any $n \in \mathbb{N}$, $\displaystyle\sum_{k=0}^{n} k = \frac{1}{2} n(n+1)$

proof: $P(0)$ is true, since for $n=0$, LHS $=0$ & RHS $=0$.

Suppose $P(n)$ is true. Then

[using the inductive hypothesis]

$$\sum_{k=0}^{n+1} k = \sum_{k=0}^{n} k + (n+1) = \frac{1}{2} n(n+1) + (n+1) = \frac{1}{2}(n+1)(n+2)$$

So $P(n+1)$ is also true. By induction, $P(n)$ is true for all $n \in \mathbb{N}$. $\square$

Theorem (Strong induction) Let $P(n)$ be a family of statements indexed by $\mathbb{N}$. Suppose (i) $P(0)$ is true, and (ii) for any $n \in \mathbb{N}$, if $P(0), P(1), \ldots, P(n)$ are true, then $P(n+1)$ is true. Then $P(n)$ is true for all $n \in \mathbb{N}$.

proof: Define $Q(n)$ to be the statement '$P(k)$ is true for $k = 0, 1, \ldots, n$'. Then we know that (i) $Q(0)$ is true, and (ii) for any $n \in \mathbb{N}$, if $Q(n)$ is true, then $Q(n+1)$ is true, so by induction, $Q(n)$ is true for all $n \in \mathbb{N}$.

Hence $P(n)$ is true for all $n \in \mathbb{N}$. $\square$

<u>Proposition</u>: Every natural number greater than 1 can be expressed as a product of one or more primes.

<u>Proof</u>: Let $P(n)$ be the statement that n can be expressed as a product of primes.

$P(2)$ is true since 2 is itself prime.

Let $n > 2$, and suppose that $P(m)$ holds for all $m < n$.

If n is prime, then $P(n)$ is true. If n is not prime, then $n = rs$ for some $r, s \in \mathbb{N}$, with $r, s < n$. By inductive hypothesis, r and s can be expressed as products of primes, and hence so can $n = rs$. So $P(n)$ is true.

By strong induction, $P(n)$ holds for all $n \in \mathbb{N}$.

$\square$

Lecture 1b

Definition (addition on $\mathbb{N}$) Define addition by the rules that, for any $m \in \mathbb{N}$,

(i) $m + 0 = m$

(ii) for any $n \in \mathbb{N}$, $m + (n+1) = (m+n) + 1$

Proposition Addition is <u>associative</u>, i.e. for any $x, y, z \in \mathbb{N}$

$$x + (y+z) = (x+y) + z \quad (*)$$

proof: we induct on z. For $z = 0$,

$$\begin{aligned} LHS = x + (y+0) &= x + y && \text{[using (i) from the defn]} \\ &= (x+y) + 0 = RHS \end{aligned}$$

Suppose $(*)$ holds for $z = n$. Then for $z = n+1$,

$$\begin{aligned} LHS = x + (y+(n+1)) &= x + ((y+n)+1) && \text{[using (ii) from the defn]} \\ &= (x + (y+n)) + 1 && \text{"} \\ &= ((x+y)+n) + 1 && \text{[using inductive hypothesis]} \\ &= (x+y) + (n+1) = RHS \end{aligned}$$

So $(*)$ holds for $z = n+1$. By induction, $(*)$ holds for all $z \in \mathbb{N}$.

<u>Proposition</u> (well-ordering property of the natural numbers)

Every non-empty subset of $\mathbb{N}$ has a least element.

<u>proof</u>: Assume, for a contradiction, that S is a non-empty subset of $\mathbb{N}$ that does not have a least element. Consider $S^* = \{n \in \mathbb{N} ; n \notin S\}$.

Note that $0 \in S^*$, since $0 \notin S$ else it would be the least element.

If $0, 1, \dots, n \in S^*$, then $n+1 \notin S$, else it would be the least element. So $n+1 \in S^*$

By strong induction, $n \in S^*$ for all $n \in \mathbb{N}$. Hence S is empty, a contradiction. $\#$

$\square$

Lecture 2a

The binomial theorem & an introduction to sets

Definition For $n, k \in \mathbb{N}$, we define binomial coefficient as

$$\binom{n}{k} = {}^nC_k = \frac{n!}{(n-k)!\,k!} \quad \text{for } 0 \le k \le n \qquad \left[\binom{n}{k} = 0 \text{ for } k > n \right]$$

[Note: $0! = 1$]

These appear in Pascal's triangle

$n=0$	1
$n=1$	1 1
$n=2$	1 2 1
$n=3$	1 3 3 1

Lemma Let $n, k \in \mathbb{N}$ with $1 \le k \le n$, then

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$$

proof: $\text{LHS} = \dfrac{n!}{(n-k+1)!\,(k-1)!} + \dfrac{n!}{(n-k)!\,k!} = \dfrac{n!\,(\cancel{k} + n - \cancel{k} + 1)}{(n-k+1)!\,k!} = \dfrac{(n+1)!}{(n+1-k)!\,k!} = \text{RHS}$ $\square$

Theorem (binomial theorem). Let x, y be real or complex numbers, and let $n \in \mathbb{N}$. Then

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

proof: We use induction on n.

For $n=0$, LHS $= 1$ & RHS $= 1$, so true for $n=0$.

Suppose true for n, and consider $n+1$,

$$(x+y)^{n+1} = (x+y)(x+y)^n = (x+y) \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \quad \text{[inductive hypothesis]}.$$

$$= \sum_{k=0}^{n} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n+1-k}$$

$$= x^{n+1} + \sum_{\substack{\hat{k}=0 \\ \hat{k}=k-1}}^{n-1} \binom{n}{\hat{k}} x^{\hat{k}+1} y^{n-\hat{k}} + \sum_{k=1}^{n} \binom{n}{k} x^k y^{n+1-k} + y^{n+1}$$

$$= x^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k-1} x^k y^{n+1-k} + \binom{n}{k} x^k y^{n+1-k} \right] + y^{n+1}$$

$$= x^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} x^k y^{n+1-k} + y^{n+1} \qquad \text{[using the lemma]}.$$

$$= \sum_{k=0}^{n+1} \binom{n+1}{k} x^k y^{n+1-k} = RHS$$

By induction, the result holds for all $n \in \mathbb{N}$. $\square$

Lecture 2b

A set is a collection of objects. The objects are called the <u>elements</u> or <u>members</u>.

We write the set with elements $a_1, a_2, \ldots, a_n$ as $\{a_1, a_2, \ldots, a_n\}$.

<u>Definition</u> A is a subset of S if every element of A is an element of S. We write $A \subseteq S$.

If $A \neq S$, it is called a <u>proper subset</u>.

<u>Definition</u> The empty set $\emptyset$ is the set with no elements.

<u>Examples</u>

- $\{n \in \mathbb{N} : n \text{ divisible by } 2\} \subseteq \mathbb{N}$ is the set of even natural numbers.
- $\mathbb{Z}$ is the set of integers $\{0, \pm 1, \pm 2, \ldots\}$
- $\mathbb{Q}$ is the set of rational numbers $\{\frac{m}{n} : m, n \in \mathbb{Z}, n > 0\}$
- $\mathbb{R}$ is the set of real numbers.
- $\mathbb{C}$ is the set of complex numbers $\{a + ib : a, b \in \mathbb{R}\}$ where $i = \sqrt{-1}$
- $M_{mn}(\mathbb{R})$ is the set of m by n matrices with real coefficients.
- {🙂, 🙁}

We also have <u>intervals</u> (subsets of $\mathbb{R}$): if $a, b \in \mathbb{R}$ with $a \leq b$

$$(a,b) = \{x \in \mathbb{R} : a < x < b\} \qquad [a,b] = \{x \in \mathbb{R} : a \leq x \leq b\}$$

$$(a,\infty) = \{x \in \mathbb{R} : x > a\} \qquad (-\infty, b] = \{x \in \mathbb{R} : x \leq b\}$$

<u>Definition</u> The <u>power set</u> of a set A, denoted $\mathcal{P}(A)$, is the set of all subsets of A.

eg. $A = \{0,1\}$. Then $\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$

<u>Remark</u> Note that a is not the same thing as $\{a\}$.

We can combine two elements a, b as an <u>ordered pair</u> (a, b).

If $a, b \in \mathbb{R}$, this is just a vector.

<u>Definition</u> Given sets A and B, the <u>Cartesian product</u> $A \times B$ is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$. If $B = A$, then we write $A \times A = A^2$

eg. If $A = \mathbb{R}$, then the Cartesian product is $\mathbb{R}^2$, the set of all points on a plane.

More generally, $A_1 \times A_2 \times \dots \times A_n$ is the set of all ordered n-tuples $(a_1, a_2, \dots, a_n)$.

If A_i are all the same, we write this as A^n.

<u>Warning</u> (Russell's paradox) Suppose we try to define the set

$$H = \{ \text{sets } S : S \notin S \}$$

If $H \in H$, then by definition of H, $H \notin H$ ※

If $H \notin H$, then it satisfies the condition such that $H \in H$ ※

Lecture 3

Algebra of sets, truth tables, cardinality

Definitions Given subsets A and B of a set S, we define

- the *union* $A \cup B = \{x \in S : x \in A \text{ or } x \in B\}$
- the *intersection* $A \cap B = \{x \in S : x \in A \text{ and } x \in B\}$
- the *complement* $A^c = \{x \in S : x \notin A\}$
- the *set difference* $A \setminus B = \{x \in A : x \notin B\}$

Definition Two sets are *disjoint* if $A \cap B = \emptyset$.

If $\{A_i\}$ is a family of subsets, indexed by $i \in I$ (eg. a subset of $\mathbb{N}$), then

$$\bigcup_{i \in I} A_i = \{x \in S : x \in A_i \text{ for some } i \in I\} \qquad \bigcap_{i \in I} A_i = \{x \in S : x \in A_i \text{ for all } i \in I\}$$

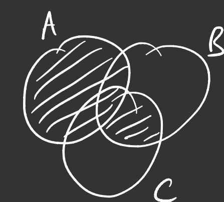
Proposition (double inclusion) For two sets $A, B \subseteq S$

$$A = B \text{ if and only if } A \subseteq B \text{ and } B \subseteq A$$

proof. Suppose $A = B$. Then every element of A is an element of B. So $A \subseteq B$. Similarly, $B \subseteq A$.

Conversely, suppose $A \subseteq B$ and $B \subseteq A$. For any $x \in S$, if $x \in A$, then since $A \subseteq B$, $x \in B$. If $x \notin A$, then since $B \subseteq A$, $x \notin B$. So the elements of A and B are the same. i.e. $A = B$. $\square$

Proposition (distributive laws) Let $A, B, C \subseteq S$. Then



(i) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(ii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

proof of (i): Suppose $x \in LHS$. Then $x \in A$ or $(x \in B$ and $x \in C)$. In either case, $x \in A \cup B$ and $x \in A \cup C$, so $x \in RHS$. i.e. $LHS \subseteq RHS$.

Conversely, suppose $x \in RHS$. Then $x \in A \cup B$ and $x \in A \cup C$. Either $x \in A$, or, if $x \notin A$ then $x \in B$ and $x \in C$ (and therefore $x \in B \cap C$). Hence $x \in A \cup (B \cap C) = LHS$.

So $\underset{RHS}{\cancel{LHS}} \subseteq \underset{LHS}{\cancel{RHS}}$. Hence, by double inclusion, $LHS = RHS$ $\square$

Proposition (De Morgan's laws) Let A, B be subsets of S. Then

(i) $(A \cup B)^c = A^c \cap B^c$

(ii) $(A \cap B)^c = A^c \cup B^c$

proof of (i): Suppose $x \in (A \cup B)^c$. Then x is not in either A or B, so $x \in A^c$ and $x \in B^c$, so $x \in A^c \cap B^c$.

Conversely, suppose $x \in A^c \cap B^c$. Then $x \notin A$ and $x \notin B$, so x is in neither A nor B. Hence $x \notin A \cup B$. ie. $x \in (A \cup B)^c$.

By double inclusion $(A \cup B)^c = A^c \cap B^c$. $\square$

De Morgan's laws extend to families of sets:

$$\left(\bigcup_{i \in I} A_i\right)^c = \bigcap_{i \in I} A_i^c \quad \& \quad \left(\bigcap_{i \in I} A_i\right)^c = \bigcup_{i \in I} A_i^c$$

Lecture 3b

Truth tables

These provide an alternative method for proving set identities.

A	B	$A \cup B$
F	F	F
F	T	T
T	F	T
T	T	T

We put T/F in the table to catalogue the different cases of whether a given element is in or out of each set.

We can use this to prove De Morgan's law $(A \cap B)^c = A^c \cup B^c$

A	B	$A \cap B$	$(A \cap B)^c$	A^c	B^c	$A^c \cup B^c$
F	F	F	T	T	T	T
F	T	F	T	T	F	T
T	F	F	T	F	T	T
T	T	T	F	F	F	F

The fact that these two columns are the same shows that these two sets are equal.

Definition (finiteness and cardinality for finite sets)

$\emptyset$ is finite and has cardinality $|\emptyset| = 0$. A set S is finite with cardinality $|S| = n+1$ if there exists an element $s \in S$ such that $|S \setminus \{s\}| = n$ for some $n \in \mathbb{N}$. Otherwise the set S is said to be infinite.

It follows that $|S|$ is the number of distinct elements in S.

[eg. $S = \{ \frac{m}{n} : m, n \in \mathbb{Z},\ 0 < m, n \leq 10^6 \}$ is finite, and $|S| = ?$]

Proposition Let A, B be finite sets. Then $|A \cup B| = |A| + |B| - |A \cap B|$.

Proof: see problem sheet.

Proposition (subsets of a finite set). Let A be a finite set, with $|A| = n$. Then $|P(A)| = 2^n$.

Proof. We use induction.

For $n = 0$, $A = \emptyset$, and $P(\emptyset) = \{\emptyset\}$, which has $|P(\emptyset)| = 1 = 2^0$.

Suppose the result holds for n, and let A have $|A| = n+1$.

Then there exists some $a \in A$ such that $A \setminus \{a\} = A'$ has cardinality $|A'| = n$.

Any subset of A either contains a or not. So we can write

$P(A) = P(A') \cup \{S \cup \{a\} : S \in P(A')\}$. These two sets are disjoint, and each has cardinality $|P(A')| = 2^n$, by the inductive hypothesis.

Hence $|P(A)| = 2^n + 2^n = 2^{n+1}$.

By induction, the result holds for all $n \in \mathbb{N}$. $\square$

For infinite sets, note $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$, but $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| < |\mathbb{R}|$

Lecture 4

Logical notation, relations, and equivalence relations

We deal with lots of logical statements or assertions, eg.

P: '$n=2$'

Q: 'n is even'

R: 'there exists $x, y, z \in \mathbb{Z}^+$ such that $x^3+y^3=z^3$.'

We can combine statements, or negate statements:

$P \vee Q$ means 'P or Q' eg. 'n is even'

$P \wedge Q$ means 'P and Q' '$n=2$'

$\neg P$ means 'not P' '$n \neq 2$'

There is a direct analogy between 'or', 'and', and 'not', and 'union', 'intersection' and 'complement', and they therefore obey De Morgan's laws:

(i) not (P or Q) = (not P) and (not Q)

(ii) not (P and Q) = (not P) or (not Q).

We write $P \Rightarrow Q$ to mean 'P implies Q', or 'If P then Q'.

We write $P \Leftrightarrow Q$ to mean $P \Rightarrow Q$ and $Q \Rightarrow P$, or 'P if and only if Q', or 'P is equivalent to Q'. Some people write 'iff'.

We write $\forall$ to mean 'for all' (eg. $\forall n \in \mathbb{N}$), or 'for every'. - the <u>universal quantifier</u>

We write $\exists$ to mean 'there exists' (eg. $\exists x \in \mathbb{R}$ s.t. $x^2 = 4$) - the <u>existential quantifier</u>

We write $\exists!$ to mean 'there exists unique' (eg. $\exists! x \in \mathbb{R}$ s.t. $x^2 = 0$)

<u>Proof</u> of the double inclusion principle ($A = B \Leftrightarrow A \subseteq B$ and $B \subseteq A$).

$$
\begin{aligned}
A = B &\Leftrightarrow \forall x \in S \ (x \in A \Leftrightarrow x \in B) \\
&\Leftrightarrow \forall x \in S \ (x \in A \Rightarrow x \in B \text{ and } x \in B \Rightarrow x \in A) \\
&\Leftrightarrow A \subseteq B \text{ and } B \subseteq A
\end{aligned}
$$

$\square$

Lecture 4b

Definition A relation R on sets A and B is a subset of $A \times B$. If $(a,b) \in R$, we write aRb. (Often $A = B$)

Example If $A = B = \{1,2,3\}$. Then

$$\leq \; = \{(1,1), (1,2), (1,3), (2,2), (2,3), (3,3)\}$$

$$\text{`}=\text{'} = \{(1,1), (2,2), (3,3)\}$$

If S is the set of students at Oxford, and C is the set of colleges, then we define R such that for any $s \in S, c \in C$, $sRc \iff s$ is a member of c.

Definitions Let S be a set and R a relation on S. Then

(i) R is <u>reflexive</u> if xRx for all $x \in S$.

(ii) R is <u>symmetric</u> if whenever xRy then yRx for all $x, y \in S$ $[\forall x,y \in S, xRy \Rightarrow yRx]$

(iii) R is <u>anti-symmetric</u> if whenever xRy and yRx then $x = y$.

(iv) R is <u>transitive</u> if whenever xRy and yRz then xRz.

Examples $\leq$ on $\mathbb{R}$ is reflexive, not symmetric, is anti-symmetric, and is transitive.

$\neq$ on $\mathbb{R}$ is not reflexive, is symmetric, not anti-symmetric, and not transitive

Definition A relation R is called a partial order if it is reflexive, anti-symmetric and transitive.

It's called a total order if for any $x, y \in S$, either xRy or yRx.

(eg. 'divides' on $\mathbb{N}$ - denoted '$|$' - is an example of a partial order that is not a total order)

Example Let $n \geq 2$, and define R on $\mathbb{Z}$ by $aRb \iff b-a$ is a multiple of n.

This is congruence modulo n

R is reflexive, and symmetric, and transitive

$$\left(\begin{aligned} aRb \text{ and } bRc &\Rightarrow b-a = kn \text{ and } c-b = ln \text{ for some } k, l \in \mathbb{Z} \\ &\Rightarrow c-a = (k+l)n \Rightarrow aRc \end{aligned} \right)$$

Definition A relation R on a set S is an <u>equivalence relation</u> if it is reflexive, symmetric and transitive. In this case, we write it as $\sim$

Examples $S = \mathbb{Z}$, and $\sim$ is congruence modulo n (we write $a \sim b$ as $a \equiv b \mod n$)

$S = \mathbb{C}$ and $z \sim w \iff |z| = |w|$

$S = \{\text{set of polygons in } \mathbb{R}^2\}$ and $\sim$ is congruence.

$S = M_n(\mathbb{R})$ is the set of $n \times n$ matrices with real coefficients, and $\sim$ is similarity of matrices ($A \sim B \iff \exists$ an invertible matrix P s.t. $A = P^{-1}BP$)

Definition Given an equivalence relation $\sim$ on a set S, and given an element $x \in S$, we define <u>equivalence class</u> of x as

$$\bar{x} = \{y \in S : y \sim x\}$$

Definition A partition of a set S is a collection of non-empty disjoint subsets, whose union is S.

$$\left(\{A_i : i \in I\} \text{ such that } A_i \neq \emptyset \text{ for all } i \in I, \ \bigcup_{i \in I} A_i = S, \text{ and } A_i \cap A_j = \emptyset \text{ for } i \neq j \right)$$

Given a partition of a set S, we can define an equivalence relation $\sim$ by saying that $x \sim y \iff x$ and y are in the same part of the partition.

Example If S is the set of Oxford students, we can partition according to colleges, and then $x \sim y$ if x and y are at the same college.

Proposition Given an equivalence relation $\sim$ on a set S, the equivalence classes form a partition of S.