Ch 3.

Relations & functions

- The extension of a property $P(x), x \in U$, is a set \{ $x \in U \mid P(x)$ \}.

What is the extension of a property $P(x, y), x \in U, y \in V$, or $P(x, y, z), x \in U, y \in V, z \in W$?

- In the 19c. it was recognised that functions were often, but not always, associated with expressions eg. $x^2 + 3$ for $x \in \mathbb{R}$. 
Pairs & Products

\{a, b\} unordered pair of \(a, b\).

\((a, b)\) ordered pair of \(a, b\).

\((a, b) = (a', b') \iff a = a' \& b = b'\).

We could define \((a, b) = \{\{a\}, \{a, b\}\}\).

The product of sets \(X\) and \(Y\)

\(X \times Y = \{\{a, b\} \mid a \in X \& b \in Y\}\).

E.g.

\(\mathbb{R} \times \mathbb{R}\)
Some laws:

\[ A \times (B \cup C) = (A \times B) \cup (A \times C) \]
\[ A \times (B \cap C) = (A \times B) \cap (A \times C) \]
\[ (A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D) \]
\[ (A \times B) \cup (C \times D) \leq (A \cup C) \times (B \cup D) \]
Some laws:

\[ A \times (B \cup C) = (A \times B) \cup (A \times C) \]
\[ A \times (B \cap C) = (A \times B) \cap (A \times C) \]
\[ (A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D) \]
\[ (A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D) \]
A binary relation between sets $X, Y$ is a subset $R \subseteq X \times Y$.

$(x, y) \in R$ often written $x \mathrel R y$.

E.g.,
\[
\{ (x, y) \in R \times R \mid x < y \}
\]

\[
\{ (x, y) \mid x \text{ is parent of } y \} \subseteq P \times P
\]

$P$ is set of people
A function from a set $X$ to set $Y$ is a relation $f \subseteq X \times Y$ such that:

1. $(x, y) \in f \& (x, y') \in f \Rightarrow y = y'$ for all $x \in X$, $y, y' \in Y$;

2. $\forall x \in X \ \exists y \in Y. \ (x, y) \in f$

Write $f(x)$ for the unique $y$ s.t. $(x, y) \in f$.

A partial function from $X$ to $Y$ is a relation $f \subseteq X \times Y$ s.t. (1).
A function from a set $X$ to set $Y$ is a relation $f \subseteq X \times Y$ such that:

1. $(x, y) \in f$ & $(x, y') \in f \Rightarrow y = y'$ for all $x \in X$, $y, y' \in Y$;

2. $\forall x \in X \exists y \in Y. (x, y) \in f$

Write $f(x)$ for the unique $y$ s.t. $(x, y) \in f$.

A partial function from $X$ to $Y$ is a relation $f \subseteq X \times Y$ s.t. (1).
Composing relations and functions.

\[ R \subseteq X \times Y \quad S \subseteq Y \times Z \]

Their composition:

\[ S \circ R = \{ (x,z) \in X \times Z \mid \exists y \in Y. \ (x,y) \in R \land (y,z) \in S \} \]

Identity:

\[ \text{id}_X \subseteq X \times X \]

\[ \text{id}_X = \{ (x,x) \mid x \in X \} \]

Associativity:

\[ R \subseteq X \times Y, \ S \subseteq Y \times Z, \ T \subseteq Z \times W \]

\[ T \circ (S \circ R) = (T \circ S) \circ R \]
Composing relations and functions.

\[ R \subseteq X \times Y \quad S \subseteq Y \times Z \]

Their composition:

\[ S \circ R = \{ (x,z) \in X \times Z \mid \exists y \in Y. (x,y) \in R \land (y,z) \in S \} \]

Identity:

\[ \text{id}_x \subseteq X \times X \]

\[ \text{id}_x = \{ (x,x) \mid x \in X \} \]

Associativity:

\[ R \subseteq X \times Y, \quad S \subseteq Y \times Z, \quad T \subseteq Z \times W \]

\[ T \circ (S \circ R) = (T \circ S) \circ R \]

Composition of functions/partial funs is a function/partial function.
Special functions

Let \( f : X \rightarrow Y \).

\( f \) is injective (1-1) iff
\[ \forall x, x' \in X. \quad f(x) = f(x') \Rightarrow x = x' \]

\( f \) is surjective (onto) iff
\[ \forall y \in Y \exists x \in X. \quad y = f(x). \]

\( f \) is bijective (1-1 correspondence) iff
\( f \) is injective and surjective.

Proposition 3.9

\( f : X \rightarrow Y \) is bijective iff it has an inverse
i.e. \( g : Y \rightarrow X \) s.t. \( g(f(x)) = x \) for all \( x \in X \)
and \( f(g(y)) = y \) for all \( y \in Y. \)
Special functions

Let $f : X \rightarrow Y$.

$f$ is injective (1-1) iff
\[ \forall x, x' \in X. \quad f(x) = f(x') \Rightarrow x = x', \]

\[ \text{injective function} = \text{injection} \]

$f$ is surjective (onto) iff
\[ \forall y \in Y \exists x \in X. \quad y = f(x). \]

\[ \text{surjective function} = \text{surjection} \]

$f$ is bijective (1-1 correspondence) iff
$f$ is injective and surjective.

\[ \text{bijective fn.} = \text{bijection} \]

**Proposition 3.9**

$f : X \rightarrow Y$ is bijective iff it has an inverse

ie. $g : Y \rightarrow X$ s.t.
\[ g(f(x)) = x \text{ for all } x \in X \]
and
\[ f(g(y)) = y \text{ for all } y \in Y. \]
Direct and inverse image

\[ R \subseteq X \times Y \]

Let \( A \subseteq X \). Its direct image under \( R \)

\[ RA = \{ y \in Y \mid \exists x \in A. \ (x, y) \in R \} \]

Let \( B \subseteq Y \). Its inverse image under \( R \)

\[ R^{-1}B = \{ x \in X \mid \exists y \in B. \ (x, y) \in R \} \]
Partitions:
- \( x \in \{x^3_R \} \)
- \( \{x^2_R \} \cap \{y^2_R \} \neq \emptyset \Rightarrow \{x^2_R \} = \{y^2_R \} \)

(1) \( \{x^2_R \} \cap \{y^2_R \} \neq \emptyset \Rightarrow xRy \)

(2) \( xRy \Rightarrow \{x^2_R \} = \{y^2_R \} \)
Examples of equivalence relations

- For $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$
  \[ a \equiv b \mod m \]
  iff $m$ divides $a - b$
  ie. $a$ and $b$ have same remainder when divided by $m$. [Ex. 3.18]

- ‘Sameness’ relations
  Eg. In this class
  ‘$x$ and $y$ have the same age’
  ‘$x$ and $y$ have the same college’

- Equivalences on states of computation:
  bisimulation [Ex. 3.20], ...
Equivalence relations.

An equivalence relation on a set $X$ is a relation $R \subseteq X \times X$ which is:

- reflexive: $\forall x \in X. \ x R x$
- symmetric: $\forall x, y \in X. \ x R y \Rightarrow y R x$
- transitive: $\forall x, y, z \in X. \ x R y \& y R z \Rightarrow x R z$

Let $x \in X$. Its equivalence class

$$\{ x^2_R \} = \{ y \in X \mid y R x \}$$

**Theorem 3.13**

\[ \{ \{ x_R \mid x \in X \} \} \text{ is a partition of the set } X. \]
Relations as structure—other examples

Directed graphs \((X, R)\) where \(R \subseteq X \times X\).

Partial orders \((P, \leq)\) where \(\leq \subseteq P \times P\).

s.t.

refl. \(p \leq p\)

tran. \(p \leq q \& q \leq r \Rightarrow p \leq r\)

antisym. \(p \leq q \& q \leq p \Rightarrow p = q\)

Cf. \(\subseteq\) on sets

least upper bounds \(\lor\) (cf. \(U\))
greatest lower bounds \(\land\) (cf. \(\cap\))
Relations as structure - other examples

Directed graphs \((X, R)\) where \(R \subseteq X \times X\).

Partial orders \((P, \leq)\) where \(\leq \subseteq P \times P\)

s.t.
refl. \(\quad p \leq p\)
trans. \(\quad p \leq q \land q \leq r \Rightarrow p \leq r\)
antisym. \(\quad p \leq q \land q \leq p \Rightarrow p = q\)

Cf. \(\leq\) on sets & \(\subseteq\) on \(R_y\)

1. Least upper bounds \(\lor\) \((\text{cf. } R_y U)\)
greatest lower bounds \(\land\) \((\text{cf. } \cap)\)

2. Assume \(x R y\).
   Let \(z \in \{x, y\}\), i.e. \(z R x \land z R y \land z \in \{x, y\}\).
   Let \(w \in R_y \land x, y \in R_x \land w R y \land x, y \in R_x \land w R x \land w e \{x, y\}\).

Size of sets

-countability.

Two sets have the same size (or cardinality) iff there is a bijection between them.
A set $A$ is finite iff there is a bijection $f : \{m \in \mathbb{N} \mid m \leq n\} \to A$ for some $n \in \mathbb{N}_0$.

A set $A$ is countable iff $A$ is finite or there is a bijection $f : \mathbb{N} \to A$. 
Lemma 3.25 Any subset $A$ of $\mathbb{N}$ is countable.
Lemma 3.25: Any subset \( A \) of \( \mathbb{N} \) is countable.

Proof idea:

Define \( f : \mathbb{N} \rightarrow A \) by math. ind.

\( f(1) \) is least element of \( A \) if \( A \neq \emptyset \);
undefined otherwise.

\( f(n+1) \) is least element of \( A \) above \( f(n) \)
if \( f(n) \) is defined & there is
a member of \( A \) above \( f(n) \);
undefined otherwise.
The composition of injections / surjections / bijections is an injection / surjection / bijection.
The composition of injections / surjections / bijections is an injection / surjection / bijection.

\[
\begin{array}{c}
A \xrightarrow{f} B \xrightarrow{g} C
\end{array}
\]
Corollary 3.26
A set $B$ is countable iff there is a bijection $g: A \rightarrow B$ where $A \subseteq \mathbb{N}$.

Lemma 3.27
A set $B$ is countable iff there is an injection $f: B \rightarrow \mathbb{N}$.

Lemma 3.28 (VERY USEFUL!)
A set $B$ is countable iff there is an injection $f: B \rightarrow A$ where $A$ is countable.

In particular, a subset of a countable set is countable.
3.26 (only if) \[ \forall x \in A, \exists y \in B \text{ such that } (x, y) \in g \]

\[ g \circ f : D \to A \]

3.27 (only if) \[ A \to B \]

3.28 (only if) \[ f' \circ f : B \to A \to \mathbb{N} \]
Lemma 3.29  The set $\mathbb{N} \times \mathbb{N}$ is countable.

Corollary 3.30  The set $\mathbb{Q}^+$ is countable.

Lemma 3.32  Suppose $A_1, A_2, \ldots, A_n, \ldots$ are countable sets. Their union

$$\bigcup_{n \in \mathbb{N}} A_n = \{ x \mid \exists n \in \mathbb{N}. x \in A_n \}$$

is countable.
Lemma 3.29 The set $\mathbb{N} \times \mathbb{N}$ is countable.

$f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$

$f(m,n) = 2^m \times 3^n$

Corollary 3.30 The set $\mathbb{Q}^+$ is countable.

$f: \mathbb{Q}^+ \rightarrow \mathbb{N} \times \mathbb{N}$

$f(m,n) = (m, n)$

Lemma 3.32 Suppose $A_1, A_2, \ldots, A_n, \ldots$ are countable sets. Their union

$\bigcup_{n \in \mathbb{N}} A_n = \{ x \mid \exists n \in \mathbb{N}. x \in A_n \}$

is countable.

$\begin{array}{c}
A_1 \\
\vdots \\
A_n \\
\end{array}$

$\begin{array}{c}
A_1 \rightarrow \mathbb{N} \\
\vdots \\
A_n \rightarrow \mathbb{N} \\
\end{array}$

$x \in \bigcup_{n \in \mathbb{N}} A_n$ implies $x \in A_n$ for some $n \in \mathbb{N}$

$h: \bigcup_{n \in \mathbb{N}} A_n \rightarrow \mathbb{N} \times \mathbb{N}$

$h(x) = (n_x, f_{n_x}(x))$

Assume $h(x) = h(y)$.

$h(y) = (n_y, f_{n_y}(y))$

$n_x = n_y = n$ say

$f_{n_x}(x) = f_{n_y}(y)$

$x = y$ as $f_n$ is a bijection.
Cor: \( \mathbb{Z} = \{0\} \cup \mathbb{N} \cup \{-n \mid n \in \mathbb{N}\} \) is countable.
Cor. 3.31.

\[ A, B \text{ otble} \]

\[ \Rightarrow A \times B \text{ otble} \]

**Proof.**

\[ f_A : A \rightarrow \mathbb{N} \]

\[ f_B : B \rightarrow \mathbb{N} \]

\[ ? f : A \times B \rightarrow \mathbb{N} \times \mathbb{N} ? \]

\[ f(a, b) = (f_A(a), f_B(b)) \]

Suppose \( f(a, b) = f(a', b') \)

Then \( (f_A(a), f_B(b)) = (f_A(a'), f_B(b')) \)

\[ f_A(a) = f_A(a') \text{ } \& \text{ } f_B(b) = f_B(b') \]

\[ a = a' \text{ } \& \text{ } b = b' \]

\[ (a, b) = (a', b') . \]

\[ \text{ } \square \text{ } \]
Georg Cantor

Size of sets

"Diagonal argument"
Theorem 3.37 \( \mathbb{R} \) is uncountable.
Theorem 3.37: \( \mathbb{R} \) is uncountable.

Proof. By contradiction.

Assume \( \mathbb{R} \) is countable.

Then \( (0, 1] \) is countable.

\[
\begin{align*}
  f(1) &= 0. \; d_1^1 \; d_2^1 \; d_3^1 \; \ldots \; d_i^1 \; \ldots \\
  f(2) &= 0. \; d_1^2 \; d_2^2 \; d_3^2 \; \ldots \; d_i^2 \; \ldots \\
  f(3) &= 0. \; d_1^3 \; d_2^3 \; d_3^3 \; \ldots \; d_i^3 \; \ldots \\
  & \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\
  f(n) &= 0. \; d_1^n \; d_2^n \; d_3^n \; \ldots \; d_i^n \; \ldots \\
  & \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\
\end{align*}
\]
Theorem 3.37: \( \mathbb{R} \) is uncountable.

Proof: By contradiction.
Assume \( \mathbb{R} \) is countable.
Then \([0,1]\) is countable.

\[
\begin{align*}
\mathbf{f}(1) &= 0. \boxed{d_1^1} d_2^1 d_3^1 \ldots d_i^1 \ldots \\
\mathbf{f}(2) &= 0. d_1^2 \boxed{d_2^2} d_3^2 \ldots d_i^2 \ldots \\
\mathbf{f}(3) &= 0. d_1^3 d_2^3 \boxed{d_3^3} \ldots d_i^3 \ldots \\
& \vdots \quad \vdots \quad \vdots \quad \vdots \\
\mathbf{f}(n) &= 0. d_1^n d_2^n d_3^n \ldots d_i^n \ldots \\
& \vdots \quad \vdots \quad \vdots \quad \vdots \\
\mathbf{r} &= 0. \; r_1 \; r_2 \; r_3 \ldots \; r_i \ldots \\
\end{align*}
\]

\[
\begin{align*}
r_i &= \begin{cases} 
1 & \text{if } d_i^i \neq 1 \\
2 & \text{if } d_i^i = 1
\end{cases}
\end{align*}
\]
Via \( (0,1] = \{ r \in \mathbb{R} \mid 0 < r \leq 1 \} \)

is uncountable.

But: \( S = \{ s \in (0,1] \mid s \text{ can be expressed by a finite decimal} \} \)
An algebraic number is a solution to a polynomial equation

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0$$

where the coefficients $a_0, \ldots, a_n \in \mathbb{Z}$.

A transcendental is a real number which is not algebraic.

There are (uncountably many) transcendental numbers!
An algebraic number is a solution to a polynomial equation

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = 0$$

where the coefficients $a_0, \ldots, a_n \in \mathbb{Z}$.

A transcendental is a real number which is not algebraic.

There are (uncountably many) transcendental numbers!

$$\mathbb{Z} \cup \mathbb{Z} \times \mathbb{Z} \cup \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \cup \ldots$$

$$\cup \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \cup \ldots$$

$$\cup \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \cup \ldots$$

$$\cup \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \cup \ldots$$

$$\mathbb{R} = \text{Alg} \cup \text{Trans}$$

rational numbers \underline{uncountable}