Watch out for the common error of counting things twice.

We will now work with some useful relationships involving $\binom{n}{r}$.

Theorem 6. *Let n and r be positive integers with $r \leqslant n$. Then*

$$\binom{n}{r} = \binom{n}{n-r}.$$

Example 35. *Given that* $\binom{n}{2} = \dfrac{n(n-1)}{2}$, *find an expression for* $\binom{x+3}{x+1}$.

Pascal's Formula Let n and r be positive integers with $r \leqslant n$. Then

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}. \quad (3)$$

Example 36. *Use Pascal's formula* (3) *to calculate:*

(a) $\binom{7}{5} + \binom{7}{6}$

(b) $\binom{9}{6} + \binom{9}{5}$

(c) $\binom{4}{2} + \binom{4}{3}$

(d) $\binom{6}{1} + \binom{6}{2}$

2.4 Cardinality

In this section we shall investigate the concept of the *cardinality* of a set and show that there are *infinite* sets that are larger than other infinite sets. This concept has applications in determining what can and what cannot be computed on a computer.

- A **finite** set is either one which has no elements at all, or one for which there exists a one-to-one correspondence (bijection) with a set of the form $\{1, 2, 3, \ldots, n\}$ for some fixed positive integer n.
- An **infinite** set is a nonempty set for which there does *not* exist any one-to-one correspondence (bijection) with a set of the form $\{1, 2, 3, \ldots, n\}$ for any positive integer n.
- Let $\mathcal{A}$ and $\mathcal{B}$ be any sets. Sets $\mathcal{A}$ and $\mathcal{B}$ are said to have the **same cardinality** if and only if there exists a one-to-one correspondence (bijection) from $\mathcal{A}$ to $\mathcal{B}$.

  In other words, $\mathcal{A}$ has the **same cardinality** as $\mathcal{B}$ if and only if there is a function f from $\mathcal{A}$ to $\mathcal{B}$ that is one-to-one (injective) and onto (surjective).

A set of even numbers

B set of odd numbers

$A = \{2k : k \in \mathbb{Z}\}$

$B = \{2k+1 : k \in \mathbb{Z}\}$

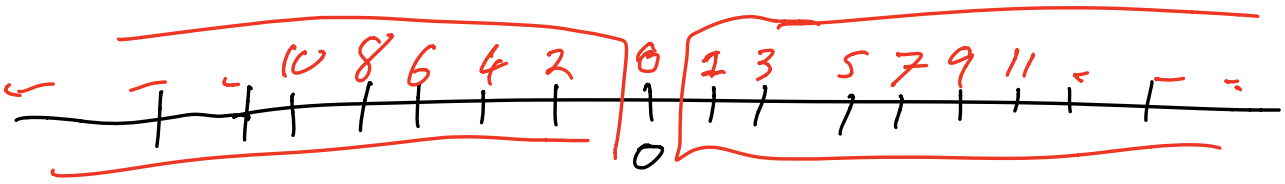
$2k-1$

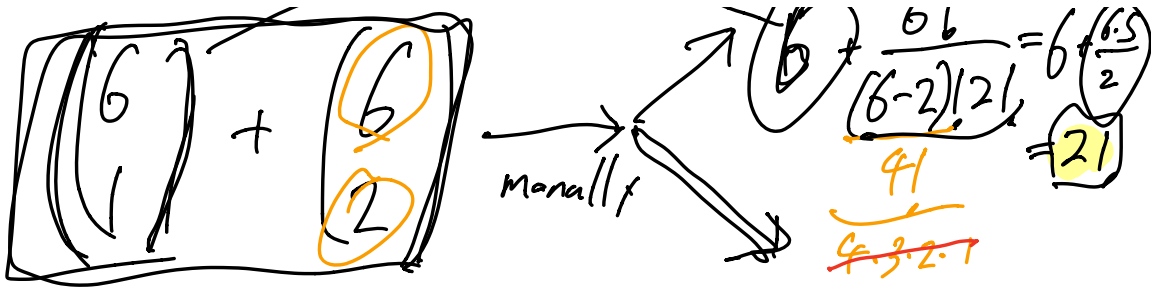
$2k+25$

$B = A \oplus 1$

$A = \mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$

$B = \mathbb{Z} = \{\ldots -2, -1, 0, 1, 2, \ldots\}$





using Pascal

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

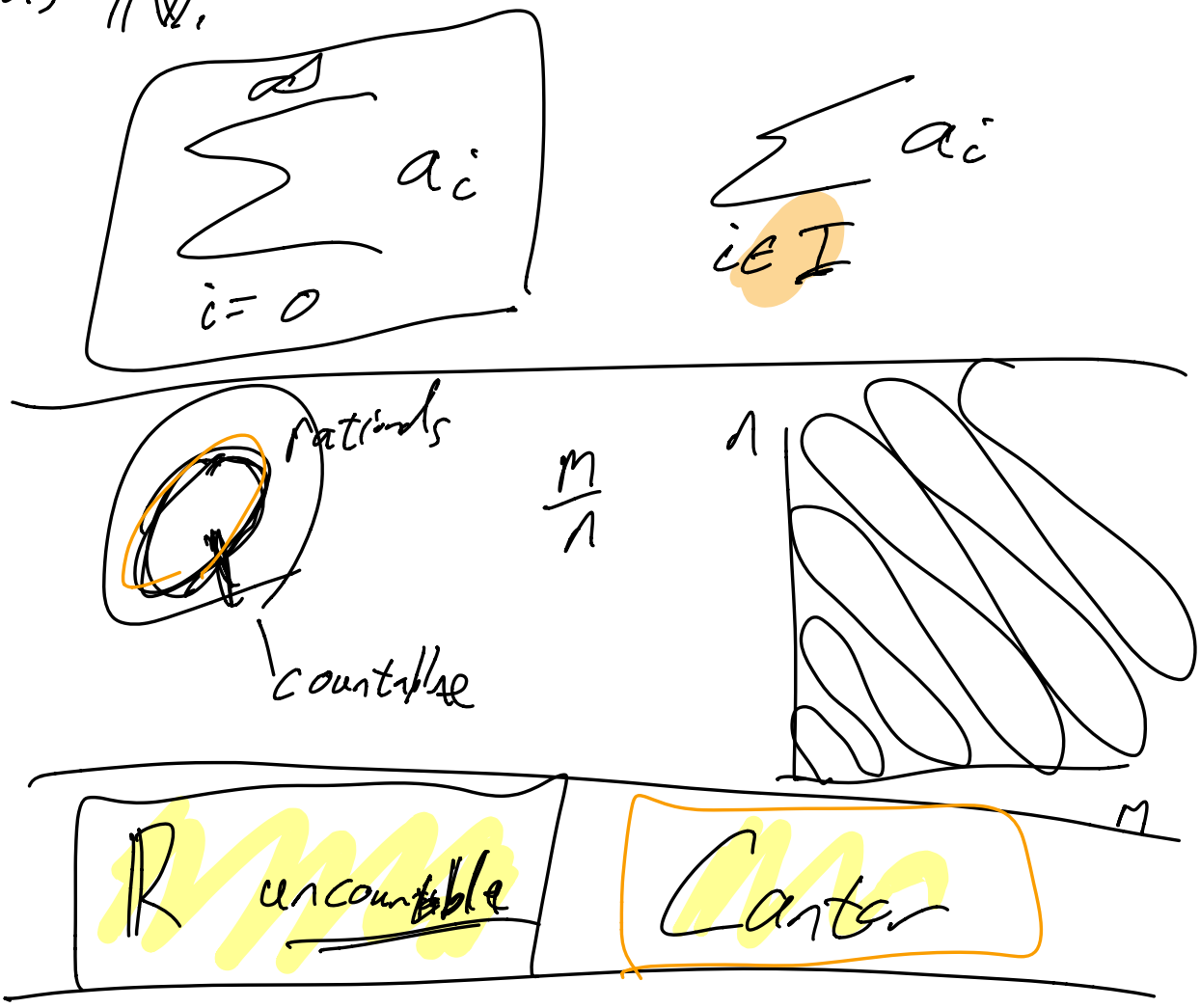
$n = 6$, $r = 2$

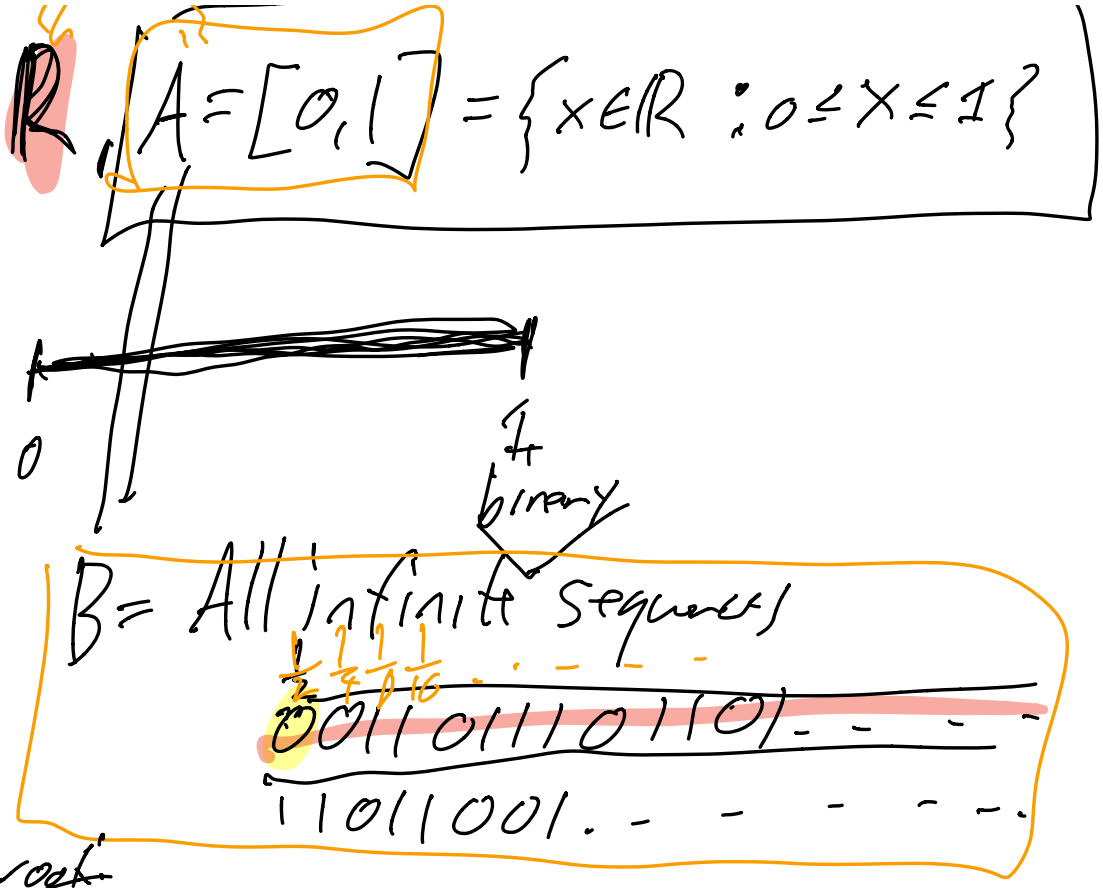
$$\binom{7}{2} = \binom{6}{1} + \binom{6}{2}$$

$r - 1 = 1$

$$\frac{7!}{5!2!} = \frac{7 \cdot 6}{2} = 7 \cdot 3 = 21$$

A set is countable if it is finite or it has the same cardinality as $\mathbb{N}$.





proof:

Assume B is countable, so enumerate it's elements:

1: 0010111011111101 . . .
2: 0001110 . . .
3: 0010011 . . .

Now Take an element a which flips every bit in the diagonal

- A set is called **countably infinite** if and only if it has the same cardinality as the set of positive integers $\mathbb{Z}^+$.
- A set is called **countable** if and only if it is finite or it is countably infinite.

Example Consider: $f : \mathbb{Z} \mapsto \mathbb{Z}^2 \qquad f(x) = x^2$

Here we can see f is surjective but not injective, so not a bijection.

Example 37. *Show that the following is bijective:* $f : \mathbb{Z}^+ \mapsto \mathbb{Z}^2 \qquad f(x) = x^2$

Start by assuming $f(x_1) = f(x_2)$. Then $x_1^2 = x_2^2$, and taking square roots gives $x_1 = x_2$ since $\mathbb{Z}^+$ contains only positive integers. To show surjective, let $x^2 \in \mathbb{Z}^2$, then $x \in \mathbb{Z}^+$ and $f(x) = x^2$.

Example 38. *The sets* $\{1, 4, 5, 6, b\}$, $\mathbb{Z}^{>0}$, $\mathbb{Z}$, *and* $\mathbb{Q}$ *are all countable.*

- A set that is not countable is called **uncountable**.

Example 39. *The sets* $\mathbb{R}$, *and* $\mathcal{P}(\mathbb{Z}(> 0))$ *are both uncountable.*

Example 40. *Show that the set of all odd integers is countable.*

Theorem 7. *Let* $\mathcal{X}$ *and* $\mathcal{Y}$ *be* **finite** *sets with the same number of elements, and suppose that* f *is a function from* $\mathcal{X}$ *to* $\mathcal{Y}$. *Then* f *is one-to-one if and only if* f *is onto.*

- This theorem does *not* hold for infinite sets of the same cardinality.

  In fact if $\mathcal{A}$ and $\mathcal{B}$ are infinite sets with the same cardinality, then there exist functions from $\mathcal{A}$ to $\mathcal{B}$ that are one-to-one and not onto, and functions from $\mathcal{A}$ to $\mathcal{B}$ that are onto and not one-to-one.

Example 41. *Given that* $\mathbb{Z}$ *has the same cardinality as the set of even integers,* $\mathbb{Z}^{even}$,

(a) *find a map from* $\mathbb{Z}^{even}$ *to* $\mathbb{Z}$ *that is one-to-one but not onto, and*

(b) *find a map from* $\mathbb{Z}$ *to* $\mathbb{Z}^{even}$ *that is onto but not one-to-one.*

Example 42. *Verify that the set* $\mathcal{P}(\mathbb{Z}^+)$ *is uncountable.*

2.5 Application: The set cover problem

3 Foundations in logic

3.1 Proof methods

In this section we will focus on the basic structure of simple mathematical proofs, and see how to disprove a mathematical statement using a counterexample.

To illustrate these proof techniques we will use the properties of *even* and *odd* integers, and of *prime* and *composite* integers.

- An integer n is **even** if and only if n is equal to two times some integer.
- An integer n is **odd** if and only if n is equal to two times some integer plus 1.
- An integer n is **prime** if and only if $n > 1$, and for all positive integers r and s, if we have $n = r \cdot s$, then $r = 1$ or $s = 1$.
- An integer is **composite** if and only if $n > 1$, and $n = r \cdot s$ for some positive integers r and s with $r \neq 1$ and $s \neq 1$.

Example 43. *Prove that for all* $x \in \{0, 1, 2, 3, 4, 5\}$, *the integer* $x^2 + x + 41$ *is a prime number.*

Method of Direct Proof:

To show that "$\forall x \in D$, if $P(x)$ then $Q(x)$" is **true**:

1. Suppose for a particular but *arbitrarily chosen* element x of D that the hypothesis $P(x)$ is true. (This step is often abbreviated "Suppose $x \in D$ and $P(x)$.")
2. Show that the conclusion $Q(x)$ is true using definitions, previously established results, and the rules for logical inference.

Example 44. *Prove that for all integers* a, b, c *and* m, *if*

$$a - b = rm \quad \textit{and} \quad b - c = sm, \quad \textit{then} \quad a - c = tm$$

for some integers r, s *and* t.

The following are common **mistakes** that are often made in proofs; they should be avoided.

- Arguing from examples.
- Using the same letter to mean two different things.
- Jumping to a conclusion.
- Begging the question (assuming the thing you are trying to prove).

- Misusing the word 'if'.

Example 45. *Consider the statement that the product of any two odd integers is an odd integer. The following "proof" of this statement is incorrect as it is 'begging the question'.*

NOT a Proof:

Suppose that m and n are odd integers.
If mn is odd, then $mn = 2k + 1$ for some integer k.

By the definition of odd, $m = 2a + 1$ and $n = 2b + 1$ for some integers a and b.

Thus $mn = (2a + 1)(2b + 1) = 2k + 1$, which is by definition odd. This is the statement which was to be shown.

Example 46. *Correctly prove the statement: the product of any two odd integers is an odd integer.*

Disproof by Counterexample:

To show that "$\forall x \in D$, if $P(x)$ then $Q(x)$" is **false**, find a value of $x \in D$ for which $P(x)$ is true and $Q(x)$ is false.

Example 47. Disprove the following statement:
If n is an even integer then $1 + 2 + 3 + \ldots + (n - 1) = kn$ for some integer k.
(Note that this statement is true for odd integers).

How to format a proof:

1. Write the theorem to be proved.
2. Clearly mark the beginning of the proof with the word "**Proof**".
3. Make your proof self-contained.
4. Write proofs in complete English sentences.
5. Conclude by stating what it is you have proved.

We continue our discussion of proof techniques now by considering the study of the rational numbers, that is, quotients of integers.

A real number is **rational** if and only if it can be expressed as a quotient of two integers with a *nonzero* denominator.

The set of all rational numbers is denoted by $\mathbb{Q}$.

A real number that is not rational is **irrational**.

$$r \text{ is rational} \iff \exists \text{ integers } a \text{ and } b \text{ such that } r = \frac{a}{b} \text{ and } b \neq 0.$$

$$O = \{2k+1 : k \in \mathbb{Z}\}$$

Claim: $m, n \in O \Rightarrow mn \in O$

Proof: $m = 2k_1 + 1$, $k_1 \in \mathbb{Z}$

$n = 2k_2 + 1$, $k_2 \in \mathbb{Z}$

$$mn = (2k_1+1)(2k_2+1) = 4k_1k_2 + 2k_1 + 2k_2 + 1$$

$$= 2(2k_1k_2 + k_1 + k_2) + 1$$

$2k_1k_2 + k_1 + k_2 \in \mathbb{Z}$

Hence $mn \in O$

Exercise

proof:

n^2 even $\Leftrightarrow$ n even

Example 48. *Determine the truth values of the following statements:*

(a) (0 is rational) $\wedge$ (0.377777 . . . is rational).

(b) ($\sqrt{7}$ is rational) $\vee$ ($\sqrt{25}$ is rational).

(c) $\forall x \in \mathbb{R}$, if $3 \leqslant x \leqslant 4$ then x is rational.

Example 49. *Prove that the product of two rational numbers is a rational number.*

Example 50. *Prove that every rational number r has an additive inverse. (In other words, prove that for every rational number r, there exists another rational number s such that $r + s = 0 = s + r$.)*

Example 51. *Prove for $a \in Q$ has a unique representative with $\gcd(p, q) = 1$.*

Example 52. *Prove that every non-zero rational number r has a multiplicative inverse.*

We now describe exactly what it means to say that one integer **divides** another integer. One of the most important theorems in number theory will also be introduced, the **Unique Factorization Theorem**.

- If n and d are integers and $d \neq 0$, then n is **divisible** by d if and only if there exists some integer k such that $n = dk$.

  Alternatively, we say that:

  n is a **multiple of** d, or

  d is a **factor of** n, or

  d is a **divisor of** n, or

  d **divides** n.

- The notation $d \mid n$ is used to represent the predicate "d divides n".

- d **does not divide** n (denoted $d \nmid n$) if and only if $\frac{n}{d}$ is not an integer.

Warning: Note the difference between "$d \mid n$" and "d/n".

Example 53. Explain your answers to the questions below:

(a) *Is it true that* $4 \mid 72$*?*

(b) *Is* 24 *a multiple of* 48*?*

(c) *Is it true that* $0 \mid 5$*?*

(d) *Is* -3 *a factor of* 9*?*

Is it true that $6 \mid 2a(3b+3)$, for all $a, b \in \mathbb{Z}$? Explain.

Is $2a(4b+1)$ a multiple of 4, for all $a, b \in \mathbb{Z}$? Explain.

- An alternative definition of a prime number is:

  An integer $n > 1$ is **prime** if and only if
  its only positive integer divisors are 1 and itself.

Theorem 8 (Unique Factorization for the Integers)**.** *Given any integer $n > 1$, there exist: a positive integer k; distinct prime numbers $p_1, p_2, \ldots, p_k$; and positive integers $e_1, e_2, \ldots, e_k$, such that*

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k},$$

and any other expression of n as a product of prime numbers is identical to this, except perhaps for the order in which the terms are written.

Example 54. *Find the unique factorization of the following integers by trial division.*

(a) 5440

(b) 43560

Suppose that k, a and b are integers.
If $k \mid a$ and $k \mid b$, prove that $k \mid (a+b)$.

Division into cases and the quotient-remainder theorem

In this section, we describe another important theorem in number theory: the **Quotient-Remainder Theorem**. We shall also encounter situations where it's easier to prove a statement by splitting the statement into cases.

Theorem 9 (Quotient-Remainder Theorem)**.** *Given any integer n and a positive integer d, there exist unique integers q and r such that*

$$n = dq + r \text{ and } 0 \leqslant r < d.$$

- Given an integer n and a positive integer d such that $n = dq + r$, where $0 \leqslant r < d$, we define

  $$n \textbf{ mod } d = r.$$

- For integers a and b, and a positive integer d, if $a \equiv r \pmod{d}$ and $b \equiv r \pmod{d}$ (so if a and b leave the same remainder upon division by d), then we say that "a is **congruent** to b **modulo** d " and write

  $$a \equiv b \pmod{d}.$$

  Note that this is the same as saying $a - b = kd$ for some integer k,
  or equivalently, $d \mid (a-b)$.

  Note: Working "$\pmod{d}$" we always assume that $d > 0$.

- If n is divisible by d, then $n \equiv 0 \pmod{d}$.

Example 55. *True or false? (Explain your answers.)*

(a) $7 \equiv 31 \pmod{6}$

(b) $-2 \equiv 8 \pmod{5}$

(c) $-27 \equiv 27 \pmod{10}$

Example 56. *Given the following values for n and d, find integers q and r such that $n = d \cdot q + r$ and $0 \leq r < d$.*

(a) $n = 102$ *and* $d = 11$.

(a) $n = -4$ *and* $d = 5$.

Example 57. *If a and b are integers such that $a = 4x + 1$ and $b = 4y + 1$ for some $x, y \in \mathbb{Z}$, then prove that the product ab is of the form $4m + 1$, for some integer m.*

Example 58. *For the positive integers u, v, w, x and d, if $u \equiv v \pmod{d}$ and $w \equiv x \pmod{d}$, prove the following two statements.*

(a) $u + w \equiv v + x \pmod{d}$.

(b) $uw \equiv vx \pmod{d}$.

Example 59. *The square of any odd integer has the form $8m + 1$ for some integer m.*

3.2 Quantified statements

SKIP

We will now extend our knowledge of symbolic representation of statements to include quantified statements, that is, statements which include words such as *every*, *each*, *some*. For example:

- *every* number is either positive or negative;
- *some* integers are perfect numbers.

Many of the examples in this section refer to sets of numbers so you need to be familiar with some common notation.

A set is usually denoted by an upper case (capital) letter, and elements of the set by lower case letters. To list the elements of a set, we use curly brackets or *braces*. For example, the set of even integers between 1 and 11 can be written as $E = \{2, 4, 6, 8, 10\}$. The symbol $\in$ is used to indicate that an element belongs to a set and the symbol $\notin$ is used to indicate that an element does not belong to a set. For example, $4 \in E$ (read "four belongs to E") and $8 \in E$, but $5 \notin E$.

- $\mathbb{Z}$ denotes the set of integers. These are the positive and negative whole numbers and zero: $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
- We use $\mathbb{Z}^+$ to denote the positive integers, $\{1, 2, 3, \ldots\}$.
- $\mathbb{Q}$ denotes the set of rational numbers. These are the numbers that can be written as a quotient of integers, a/b, where a and b are integers and b *is nonzero*. All terminating or repeating decimals are rational numbers.
- $\mathbb{R}$ denotes the set of all real numbers. This includes all the rational numbers and all the irrational numbers (non-terminating and non-repeating decimals).

A **predicate** is a sentence that contains a finite number of variables; it becomes a statement when the variables are replaced with specific values.

Example 60. *In the following, x, a and b are integers. Which of the following are predicates?*

- *x is a positive integer.*
- *Please don't eat that.*
- *a is a factor of b.*
- *2 divides x and x divides 6.*
- *My toy elephant is grey.*
- *Paul is 20 years old.*

Predicates are often denoted by an upper case letter followed by variables listed within brackets. For example, the predicate "x is a multiple of 10" might be denoted by $P(x)$.

- The **domain** of a predicate variable is the set of all values that may be substituted in place of the variable. The set of all such elements that make the predicate true is called the **truth set** of the predicate.

Example 61. *Let $Q(n)$ be the predicate:*
n is a factor of 15.
Find the truth set of $Q(n)$ if the domain of n is the set of integers $\mathbb{Z}$.

One way to make a predicate into a statement is to substitute a value for each variable. Another way is to add quantifiers.

- The symbol $\forall$ denotes "for all" (or for each, or for every), and is called the **universal quantifier**. Let $Q(x)$ be a predicate and D be the domain of x. The **universal statement**

  $$\forall\, x \in D,\ Q(x)$$

  is true if and only if $Q(x)$ is true for every x in D.
  It is false if and only if $Q(x)$ is false for at least one x in D.

Example 62. **(a)** *Translate the English sentence "All squares are rectangles" into a universal statement.*

(b) *Translate the universal statement "$\forall\, x \in \mathbb{Z},\ x \in \mathbb{R}$" into an English sentence.*

Example 63. *Determine whether the following statements are true or false.*

(a) $\forall\, x \in \mathbb{R},\ x^2 = 2$

(b) $\forall\, x \in \{1, 2, 3\},\ x^2 < 10$

- *The symbol $\exists$ denotes "there exists" (or there is, or there are), and is called the* **existential quantifier**. *Let $Q(x)$ be a predicate and D be the domain of x. The* **existential statement**

  $$\exists\, x \in D \text{ such that } Q(x)$$

  is true if and only if $Q(x)$ is true for at least one x in D. It is false if and only if $Q(x)$ is false for every x in D.

Example 64. **(a)** *Translate the English sentence "There is a real number that is also a rational number" into an existential statement.*

(b) *Let E be the set of all elephants. Translate the existential statement "$\exists\, x \in E$ such that x is white" into an English sentence.*

Example 65. *Determine whether the following statements are true or false.*

(a) $\exists\, x \in \mathbb{R}$ *such that* $x^2 = 2$

(b) $\exists\, x \in \{1, 2, 3\}$ *such that* $x > 4$

One of the most important statement forms in mathematics is:

$$\forall x,\ \text{if } P(x) \text{ then } Q(x)$$

or equivalently,

$$\forall\, x,\ (P(x) \Rightarrow Q(x))$$

Example 66. **(a)** *Rewrite the following formal statement as an English sentence.*

$$\forall\, x \in \mathbb{R},\ \textit{if } x^2 < 9 \textit{ then } x < 3.$$

(b) *Rewrite the following English sentence as a formal statement.*
If a number is an integer, then it is a rational number.

3.3 Indirect argument: contradiction and contraposition

In this section two powerful methods of proof are introduced: **contradiction** and **contraposition**.

These are very useful alternatives to the method of direct proof which we met earlier in this chapter.

Method of Proof by Contradiction:

- Assume that the statement to be proved is false.
  Recall that the negation of the statement $\forall\, x \in D$ *if* $P(x)$ *then* $Q(x)$ *is* $\exists\, x \in D$ *such that* $P(x)$ *and* $\sim Q(x)$.
- Show that this assumption leads logically to a contradiction.
- Conclude that the statement to be proved is true.

The following form of *indirect* argument is based on the logical equivalence between a statement and its contrapositive.

Method of Proof by Contraposition

- Write the statement in the form:

  $$\forall\, x \in D,\ \text{if}\ \ P(x)\ \ \text{then}\ \ Q(x).$$

- Rewrite this statement in the contrapositive form:

  $$\forall\, x \in D,\ \text{if}\ \ \sim Q(x)\ \ \text{then}\ \ \sim P(x).$$

- Prove the contrapositive by direct proof.
  - Suppose x is a particular (but arbitrarily chosen) element of D such that $Q(x)$ is false.
  - Show that $P(x)$ is false.

Example 67. *Prove the following statement by contradiction:*
For all integers n and all prime numbers p, if n^2 is divisible by p, then n is divisible by p.

Example 68. *Prove the following statement by contraposition:*
For all integers n, if n^2 is odd, then n is odd.

Example 69. *Prove the product of any nonzero rational number and any irrational number is irrational using either contradiction or contraposition.*

Example 70. *Every prime $p > 3$ satisfies $p \equiv \pm 1 \pmod 6$.*

3.4 Mathematical induction

The Principle of Mathematical Induction is an extremely useful tool for proving statements about sums of sequences, about properties of integers, and about any repeated events which can be expressed in terms of consecutive integers. We'll use it to *prove* statements involving integers n, such as:

$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$; and $2^{2n-1} + 1$ is divisible by 3.

- **Principle of Mathematical Induction**
  Let $P(n)$ be a statement defined for integers n, and let a be some fixed integer.
  (Often in examples a will be 0 or 1 or a small value)
  Suppose that:
  (1) $P(a)$ is a true statement; and
  (2) For all integers $k \geqslant a$, IF $P(k)$ is a true statement, then $P(k+1)$ is a true statement.
  Then the statement $P(n)$ is true for all integers n with $n \geqslant a$.

- In the two steps above, (1) is the **basis step** and (2) is the **inductive step**.

  In the inductive step you ASSUME that $P(k)$ is true, and then do some work and SHOW that $P(k+1)$ is true.

- The supposition that $P(k)$ is true is called the **inductive hypothesis**.

Consider the analogy of a ladder, with a series of rungs.

The bottom rung is rung number a; you check that rung a is really there. Then you assume rung k is there for some k where $k \geqslant a$, and do some work to show that rung $k+1$ is also there, so you can climb up one rung of your ladder from k to $k+1$.

And starting with $k = a$ you can climb to $a+1$, then on to $a+2$, and so on. So you can get to *any* rung starting from the bottom rung a.

Now check the details of the next worked example.

Prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$, for all integers $n \geqslant 1$.

Don't forget to mention the principle of induction at the end of the proof.

Let $P(n)$ denote the statement "$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$".

Now LHS of $P(1)$ is 1, while the RHS of $P(1)$ is $\frac{1(1+1)}{2} = 1$. So both sides equal 1, which means $P(1)$ is a true statement.

The statement $P(k)$ states $1+2+\cdots+k=\frac{k(k+1)}{2}$. We **assume** this is true (this is our **inductive hypothesis**).

The statement $P(k+1)$ states $1+2+\cdots+(k+1)=\frac{(k+1)(k+2)}{2}$.

We must show that IF $P(k)$ is true, then $P(k+1)$ is also true.

$$\begin{aligned}
\text{Now L.H.S. of } P(k+1) &= 1+2+\cdots+(k+1)\\
&= 1+2+\cdots+k+(k+1)\\
&= \frac{k(k+1)}{2}+(k+1) \text{ ($P(k)$ is assumed true)}\\
&= \frac{k(k+1)}{2}+\frac{(k+1)\cdot 2}{2}\\
&= \frac{(k+1)(k+2)}{2}\\
&= \text{R.H.S. of } P(k+1).
\end{aligned}$$

Hence $P(k+1)$ is true.

Thus, by the principle of mathematical induction, for all integers $n \geqslant 1$, we have $1+2+\cdots+n = \frac{n(n+1)}{2}$.

Example 71. *For all integers $n \geq 1$, use mathematical induction to prove that*

$$\sum_{i=1}^{n}(2i-1)=n^2.$$

Example 72. *For all integers $n \geq 1$, prove that*

$$\sum_{j=1}^{n}\frac{1}{j(j+1)}=\frac{n}{n+1}.$$

Example 73. *For all integers $t \geqslant 1$, use induction to prove that*

$$\sum_{j=1}^{t}2^{j-1}=2^t-1.$$

3.5 Logic

In this chapter we shall consider some formal *logic*. This will enable us to determine whether the conclusion of a formal argument is true or false, given various suppositions or *premises* in the argument.

We shall see how to write truth tables for compound statements.

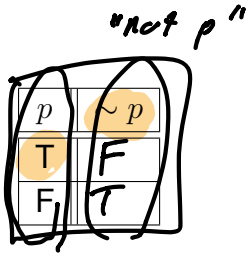
A **statement** or a **proposition** is a sentence that is true or false, but not both.

Which of the following are propositions?

- It is raining.
- Is it raining?
- Tom is a male and Susan is a female.
- Mary is a male.
- No smoking inside.
- The number 6 is a prime number.
- What comes next?
- That pelican is beautiful.
- Elizabeth's favourite bird is a pelican.
- Hello there.

- We often use p, q, r etc. to stand for simple statements.
  If we let p denote "it is raining", then we can denote the **negation** of this statement by $\sim p$ or $\neg p$. We read this as "not p", so the negation of the statement "it is raining" is "it is not raining".
- If statement p is FALSE, then what about the statement $\sim p$?
  Can you say whether it is true or false?
- A truth table gives the truth value of a statement for all possible instances of the truth values of its component parts. A statement p has two possible truth values: true or false.

Here is a truth table to complete; it will give the truth values for $\sim p$ in terms of the truth values for the statement p.



- If we have two statements, say p and q, we can combine them in various ways.
  Suppose p denotes "it is dark" and q denotes "it is raining".
  Then the statement "it is dark and it is raining" can be written as $p \wedge q$, read "p and q". This is known as the **conjunction** of p and q.
- We can use a truth table to determine the truth value of the conjunction $p \wedge q$ in all possible cases, whatever the truth values of p and q may be. With two statements p and q we have 2^2 or 4 possible scenarios.

Here is a truth table to determine the truth value of $p \wedge q$, according to the truth values of p and q.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

- The **disjunction** of two statement forms p and q, written $p \vee q$, and read "p or q", means p or q (or possibly both). This is sometimes known as the "inclusive or".

The truth table for $p \vee q$:

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

- $p \wedge q$ is true when p and q are both true.
- $p \wedge q$ is false when
- $p \vee q$ is true when
- $p \vee q$ is false when

A **statement form** or **propositional form** is made up from variables such as p, q, r, and logical connectives such as $\wedge$, $\sim$, $\vee$.

Two statement forms are **logically equivalent** if and only if they have *identical* truth values for every possible combination of truth values for the variables.

Write $P \Leftrightarrow Q$, whenever P and Q are logically equivalent.

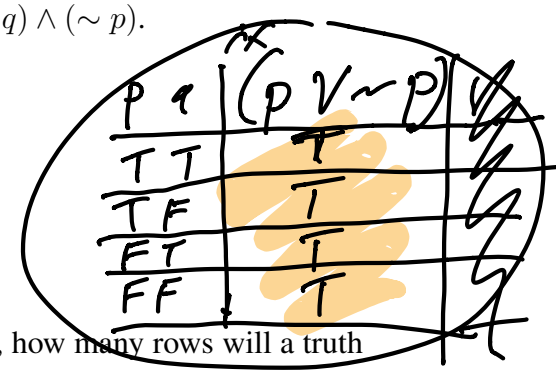
Are the statement forms $p \wedge (\sim q)$ and $(p \vee q) \wedge (\sim q)$ logically equivalent?

p	q	$p \wedge (\sim q)$	$(p \vee q) \wedge (\sim q)$
T	T	F	F
T	F	T	T
F	T	F	F
F	F	F	F

- **De Morgan's Laws** (negations of "and" and "or"):
  The statement $\sim (p \wedge q)$ is logically equivalent to the statement $(\sim p) \vee (\sim q)$.
  The statement $\sim (p \vee q)$ is logically equivalent to the statement $(\sim p) \wedge (\sim q)$.
  A **tautology** is a statement form which *always* takes the truth value TRUE, for all possible truth values of its variables.
- A **contradiction** is a statement form which *always* takes the truth value FALSE for all possible truth values of its variables.

Construct a truth table to determine the truth values for $(p \vee q) \wedge (\sim p)$.

p	q	$(p \vee q) \wedge (\sim p)$
T	T	
T	F	
F	T	
F	F	



If a statement form P has *three* variables, such as p, q and r, how many rows will a truth table for P need? Discuss.

Is the statement form
$(p \wedge q) \vee (\sim p \vee (p \wedge (\sim q)))$ a tautology, a contradiction, or neither?

p	q	$(p \wedge q) \vee (\sim p \vee (p \wedge (\sim q)))$
T	T	
T	F	
F	T	
F	F	

Practice check if taut...

The truth table for a statement form with n statement variables will have how many rows? Discuss.

When the same connective ($\wedge$ or $\vee$) is used, the commutative and associative laws hold:

Commutativity: $p \wedge q \Leftrightarrow q \wedge p$ and $p \vee q \Leftrightarrow q \vee p$.

Associativity: $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$, and $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$.

Also note the **distributive** laws:

$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$ and $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$.

Exercises:

1. Construct a truth table for $(p \vee q) \wedge \sim (p \vee r)$.
2. Exclusive or: We use $\veebar$ where $p \veebar q$ means p or q but NOT both. Write out the truth table for this exclusive or.
3. Verify one of the distributive laws with a truth table.

Conditional statements

You have probably heard the terms "if and only if" and "necessary and sufficient". In this subsection we'll examine these carefully. We'll see truth tables for "if p then q", and for "p if and only if q"; we shall see how to replace these with the logical connectives we've met already: $\vee$, $\wedge$ and $\sim$. We'll also see what the contrapositive of a statement is.

- **if** p **then** q is denoted $p \Rightarrow q$. You can also read this as "p implies q". Here p is the **hypothesis** and q is the **conclusion**.
- "if p then q" is *false* when p is TRUE and q is FALSE. It is true in *all* other cases. We'll complete the truth table for "implies":

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Translate the following statements into symbolic form. Let p denote "I will sleep", q denote "I am worried", and r denote "I will work hard".

(a) If I am worried, I will not sleep.

(b) I will not sleep if I am worried.

(c) If I am worried, then I will both work hard and not sleep.

- "If p then q" (denoted $p \Rightarrow q$) is logically equivalent to $(\sim p) \vee q$

  Check with a truth table.

p	q	$p \Rightarrow q$	$(\sim p) \vee q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Example 74. *Rewrite the following sentence in "if–then" form.*
Either you do not study or else you pass the test

- The **contrapositive** of $p \Rightarrow q$ is $\sim q \Rightarrow \sim p$.

  Saying "if p then q" is like saying "if not q, then not p".

  Again, a truth table shows this equivalence:

p	q	$p \Rightarrow q$ $\sim q \Rightarrow \sim p$
T	T	
T	F	
F	T	
F	F	

Example 75. *Write the contrapositive of the following sentence:*
If you do not study, then you will fail the test.

Example 76. *Construct a truth table to determine the truth values for* $p \Rightarrow (q \wedge (\sim p))$.

p	q	$p \Rightarrow (q \wedge (\sim p))$

There is a quote from the book *Alice in Wonderland* by Lewis Carroll (who was in fact Charles Dodgson, an English author, mathematician, logician, Anglican deacon and photographer) which is part of a conversation between Alice and the March Hare and the mad Hatter:

"Do you mean that you think you can find out the answer to it?" said the March Hare.

"Exactly so," said Alice.

"Then you should say what you mean," the March Hare went on.

"I do," Alice hastily replied; "at least—at least I mean what I say—that's the same thing, you know."

"Not the same thing a bit!" said the Hatter. "Why, you might just as well say that 'I see what I eat' is the same thing as 'I eat what I see'!"

Rewrite the statements "*I say what I mean*" and
"*I mean what I say*" in if–then format. Use a truth table to show that the two statements are not logically equivalent.

- Given statement variables p and q, the **biconditional** of p and q is $p \Leftrightarrow q$. Read this as "p if and only if q."

  $p \Leftrightarrow q$ is true precisely when p and q take the *same* truth values. It is false when p and q take opposite truth values.

  Complete its truth table:

p	q	$p \Leftrightarrow q$
T	T	
T	F	
F	T	
F	F	

- **Necessary and sufficient:**
  If p and q are statements,
  p is a **sufficient condition** for q means that if p then q.

  p is a **necessary condition** for q means that if *not* p, then *not* q.

  So if p is a **necessary condition** for q, we have: if q, then p.

Why is necessary and sufficient the same as biconditional, according to these conditions?

3.6 Application: automated reasoning

4 Relations and functions

4.1 Relations on sets

- If A and B are any sets, recall that their Cartesian product is

$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}.$$

- A **binary relation** R from a set A to a set B is any subset of $A \times B$.

  Let $(x, y) \in A \times B$. We say x *is related to* y by R, (and write $x\, R\, y$), if and only if $(x, y) \in R$.

  The notation "$(x, y) \in R$" is equivalent to the notation "$x\, R\, y$".

  If x is *not* related to y in R, we can write $x \not R\, y$ or $(x, y) \notin R$.

- Note that we often just use the word 'relation' when we mean 'binary relation', when the context is clear.

As well as using R to denote some relation, other symbols such as the Greek letters ρ (rho), σ (sigma) and τ (tau) are also often used. For example, $a\, \rho\, b$ and $c\, \tau\, d$ (means $(a, b) \in \rho$ and $(c, d) \in \tau$, respectively).

Example 77. **(a)** *Let* $A = \{0, 2, 4\}$ *and* $B = \{1, 2, 3, 4\}$.
Then $A \times B =$ _____

(b) *With* A *and* B *as above, suppose* $x\, R\, y$ *if and only if* $x \leqslant y$.

$0\, R\, 2$ *because* _____

$2\, R\, 4$ *because* _____

Since $2 \leqslant 3$ *(and* $2 \in A$, $3 \in B$*), we have* _____

We have

$R = \{$ $\}$

Example 78. *Let* $A = \{1, 2, 3, 4, 5\}$ *and* $B = \{0, 2, 4, 6, 8\}$. *In each of the following cases, suppose that* ρ *is a relation from* A *to* B*, and write down the elements in* ρ.

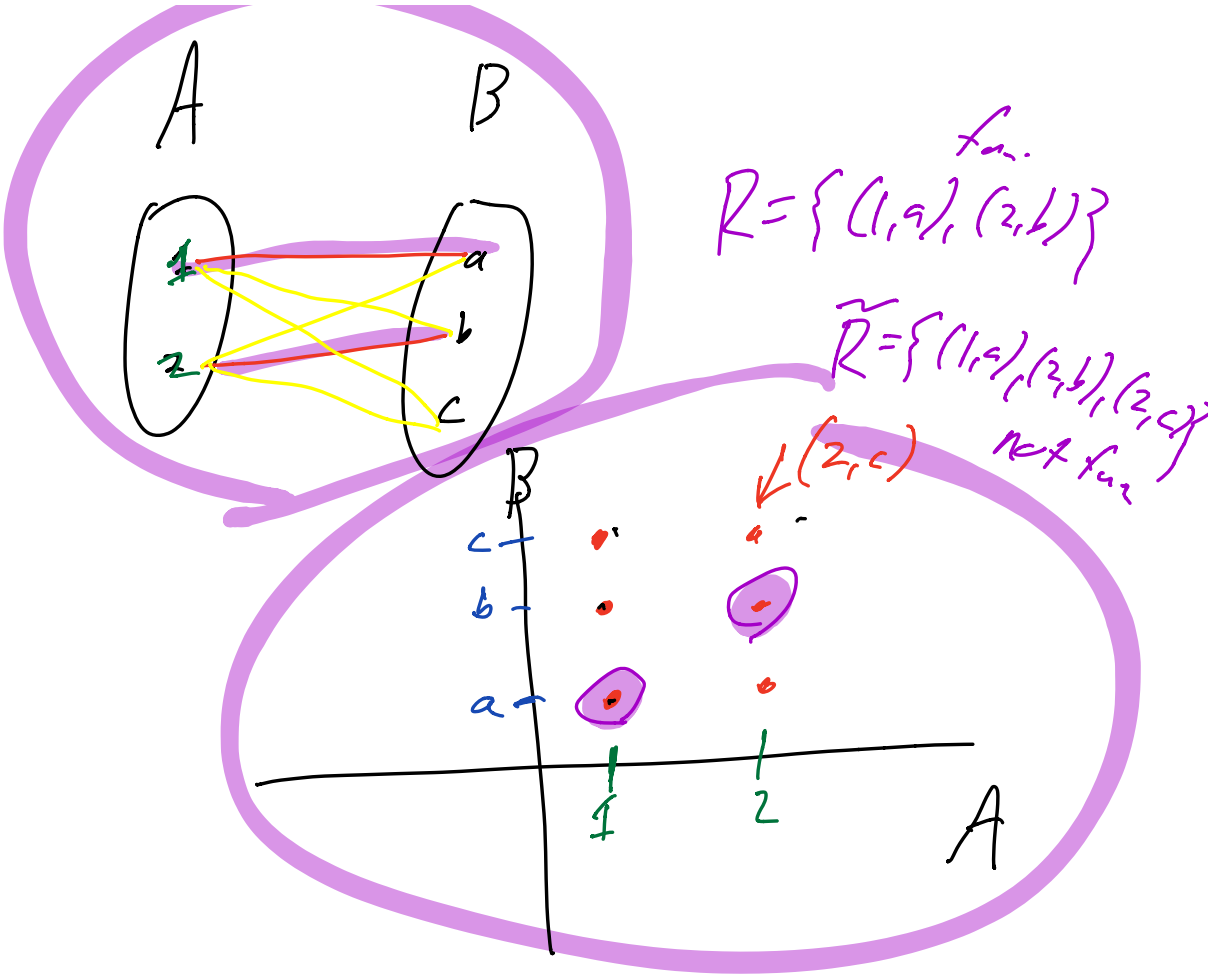
(i) $x\, \rho\, y$ *if and only if* $x \geqslant y$.

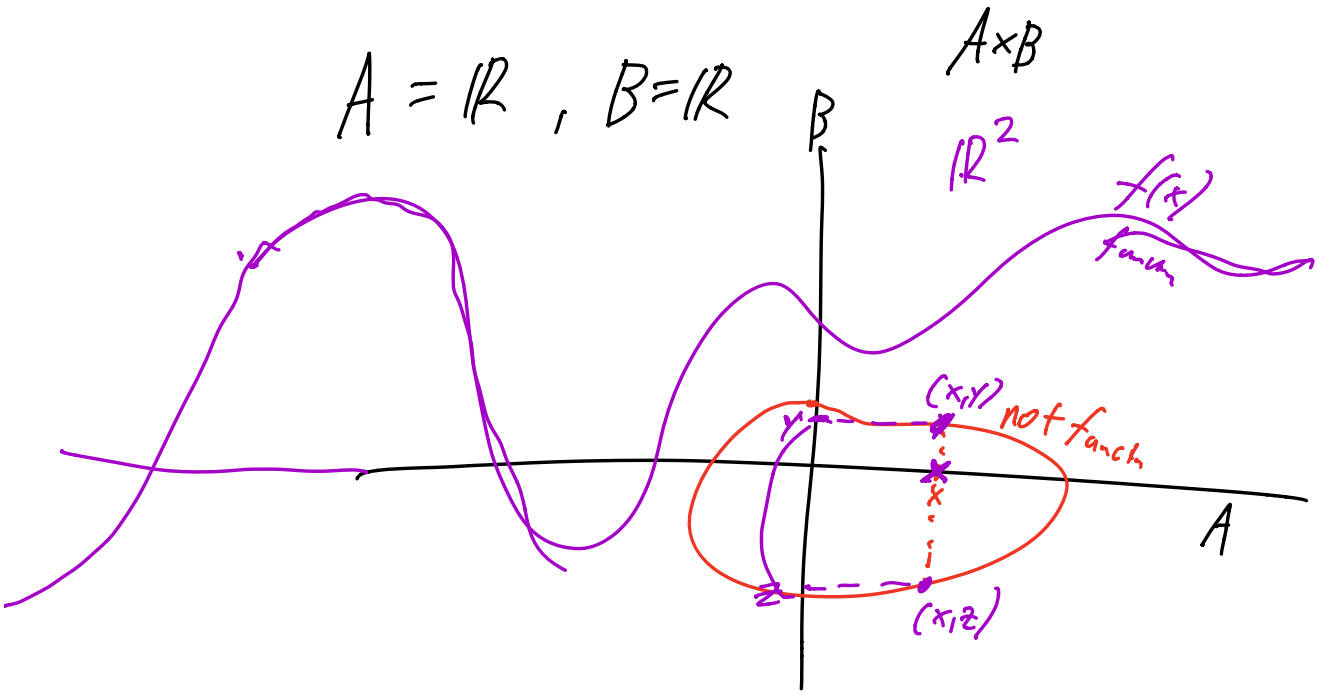
(ii) $x\, \rho\, y$ *if and only if* $x = y$.

(iii) $x\, \rho\, y$ *if and only if* $x - y$ *is even.*

(iv) $x\, \rho\, y$ *if and only if* $x + y = 7$.

(v) $x\, \rho\, y$ *if and only if* $x + y > 9$.


A
B
1
2
a
b
c
fun.
$R=\{(1,a),(2,b)\}$
$\tilde{R}=\{(1,a),(2,b),(2,c)\}$
not fun
(2,c)
B
c
b
a
1
2
A


$A=\mathbb{R}$, $B=\mathbb{R}$
$A\times B$
$\mathbb{R}^2$
B
f(x)
fun
(x,y) not fun
y
x
z
(x,z)
A

Example 79. *Define (make up) three different relations from $\mathbb{Z}$ to $\mathbb{Z}^+$, the set of positive integers. Note that there are many possible answers.*

Example 80. *Consider the following relations defined on $\mathbb{Z}$.*

(i) $R_1 = \{(a,b) : a \leqslant b\}$; **(ii)** $R_2 = \{(a,b) : a > b\}$;
(iii) $R_3 = \{(a,b) : a = b \text{ or } a = -b\}$; **(iv)** $R_4 = \{(a,b) : a = b\}$; *List some of*
(v) $R_5 = \{(a,b) : a = b + 1\}$; **(vi)** $R_6 = \{(a,b) : a + b \leqslant 3\}$.
the elements in each relation.

Example 81. *Consider each of the following ordered pairs in turn, and state which of the above relations the pair belongs to:* $(1,1),\ (1,2),\ (2,1),\ (1,-1), (2,2)$.

- **Arrow diagram:** A relation R from a set A to a set B can be represented by a directed bipartite graph G. The partite sets for the vertices of G are A and B, and for each $a \in A$ and $b \in B$, there is an arc (a directed edge) from a to b if and only if $(a,b) \in R$, that is,
  if and only if $a\,R\,b$.

Example 82. *Let $A = \{1,3,5\}$ and $B = \{1,2,3,4\}$.*
Draw a directed bipartite graph to illustrate the relation σ from A to B, where $a\,\sigma\,b$ if and only if $a + 1 > b$.

- A **function** $f : A \to B$ is a relation from the set A to the set B which satisfies:
  (i) for all $x \in A$, there exists some $y \in B$ such that $(x,y) \in f$
  (ii) for all $x \in A$ and all $y,\ z \in B$,
  $$\text{if } (x,y) \in f \text{ and } (x,z) \in f, \text{ then } y = z.$$
  If f is a function from A to B we write
  $$y = f(x) \text{ if and only if } (x,y) \in f.$$

Example 83. *Let $A = \{3,6,9\}$, $B = \{2,4,6,8\}$, and let $R = \{(3,2),\ (6,2),\ (9,6),\ (6,8)\}$ be a relation. Is R a function from A to B? Explain.*

- If R is a binary relation from A to B, then the **inverse relation**, R^{-1}, is defined from B to A by:
  $$R^{-1} = \{(y,x) \in B \times A : (x,y) \in R\}.$$

So for all $x \in A$ and $y \in B$, $(y,x) \in R^{-1}$ if and only if $(x,y) \in R$.

Example 84. *Let $A = \{x,y,z\}$ and $B = \{1,4,7,10\}$. Suppose that*
$$\rho = \{(x,4),\ (x,10),\ (z,1),\ (y,7),\ (y,1)\}$$
is a relation from A to B. Write down ρ^{-1}.