Version of 13.10.00

# MA120 Finite Mathematics

P.M.Higgins & D.H.Fremlin

This course introduces some of the mathematical ideas with which anyone studying a modern computing or mathematics degree needs to be familiar. The context in which much of modern mathematics finds itself is that of Sets, and the theory of Sets carries with it its own language which takes some getting used to. (For this reason there is a Glossary of Set Theory Symbols that will arise in the course on the back of the first problem sheet.) The underlying ideas the symbols represent are however simple. (That is not quite the same thing as saying that they are 'easy'.)

A *set* is any collection of objects referred to as *elements* or *members* of the set. Sets are generally denoted by capital letters: $A, B, S, X$ etc., while elements are usually denoted by lower case letters: $a, b, c, \cdots, x, y$ etc. The statement '$a$ is an element of $A$', '$a$ belongs to $A$', is denoted by $a \in A$; the negation of this is written $a \notin A$, '$a$ does not belong to $A$', '$a$ is not an element of $A$'. Two sets $A$ and $B$ are said to be *equal* if and only if they have the same members in which case we write $A = B$.

There are many ways of specifying sets, of which the most important are the two following methods. We may *explicitly* define a set by writing down all of its members; for example

$$A = \{-1, 1\}$$

On the other hand we may *implicitly* define a set by specifying that it consists of all objects which satisfy a certain property or properties:

$$B = \{x : x \text{is an integer and} x^2 = 1\}.$$

Note that in this case it has turned out that $A = B$. *Every set has innumerable aliases.* Just as we sometimes say '20%' and sometimes say 'one fifth', or the same person can be either 'Tony' or 'Mr Blair' or 'the Prime Minister', any particular set can appear in a wide variety of forms, and one of our little problems is to notice when an old set has turned up with a new name.

You should note the use of curly brackets when presenting a set. The set $\{1, 2\}$ is not the same as the ordered pair $(1, 2)$ (an idea that I will try to explain later). The order in which the elements happen to be listed is of no account when speaking of a set: the sets $\{Peter, Paul\}$ and $\{Paul, Peter\}$ are the same because they have the same members.

Many of the examples we shall use to illustrate ideas will involve sets of numbers because they are simple to produce but in practice, both in computing and in mathematics, the sets that people are liable to be concerned with have objects of many varied abstract kinds. They are still sets nonetheless and so questions about membership of these sets must be asked and answered using the standard terminology which we are introducing here.

Implicit definition of sets is extremely important but pre-supposes that we already have some context from which we may draw members. In most applications of set theory, and in all the questions to be treated in this course, we shall be able to identify some **universal set** $\mathcal{U}$ from which the members of all sets of interest are drawn. This 'universe' of discourse can itself vary - it depends entirely on the kind of things we may wish to consider. At the other extreme the **empty set** or **null set** is the set with no elements, denoted by $\emptyset$, or by $\{\}$. The empty set should not be confused with the number 0 (which is the number of elements in $\emptyset$).

A set $A$ is a **subset** of a set $B$ if each element of $A$ is also an element of $B$; we denote this by $A \subseteq B$ and write $A \not\subseteq B$ to say that '$A$ is not a subset of $B$', that is, there is some element of $A$ which is not a member of $B$. If $A \subseteq B$ and $A \neq B$ we say that $A$ is a *proper subset* of $B$.

---

These notes are distributed to students on the understanding that they have not been fully checked for errors. They are not intended to provide a substitute for attendance at lectures. If you notice a mistake, please tell the lecturer!

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

**Set Operations**

The **union** of two sets $A$ and $B$, denoted by $A \cup B$ (read '$A$ union $B$', '$A$ cup $B$', '$A$ join $B$') is

$$A \cup B = \{x : x \in A \mathrm{or} x \in B\}$$

We use the word 'or' to mean 'and/or', sometimes called *inclusive or*, and this is the standard usage in mathematics. When a mathematician says 'Either it's raining or it's Tuesday', you should remember that it might be both raining and Tuesday.

The **intersection** of $A$ and $B$, denoted $A \cap B$ ('$A$ intersect $B$', '$A$ cap $B$', '$A$ meet $B$'), is the set of all elements common to both sets:

$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$

**Example 1.1** $A = \{-1, 0, 1, 2\}$, $B = \{1, 2, 4\}$. Then

$$A \cup B = \{-1, 0, 1, 2, 4\}, \quad A \cap B = \{1, 2\}.$$

Note that an element is either in a set or not – it cannot be a member several times over!

The number of elements in a set $A$ is called the **cardinality** of $A$ and is denoted by $\#(A)$ or $|A|$ or $n(A)$: for instance, for the set $A$ of the above example $\#(A) = 4$, $\#(B) = 3$, $\#(A \cup B) = 5$ and $\#(A \cap B) = 2$.

The **complement** of a set $A$, denoted by $A^c$ or by $\bar{A}$ or by $\mathcal{U} \setminus A$, is the set of all elements of $\mathcal{U}$ which are *not* in $A$. For instance the complement of the set of vowels is the set of consonants (where the universal set here is, of course, the alphabet). The *difference* of sets $B$ and $A$, in that order, denoted by $B \backslash A$ or by $B - A$, '$B$ less $A$', is the set of all elements that are in $B$ but not in $A$:

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

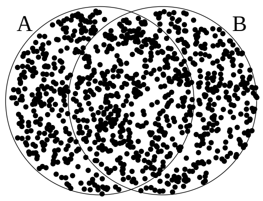
This is sometimes also called the *relative complement* of $A$ in $B$ - this is because if we take $B = \mathcal{U}$ we get $\mathcal{U} \setminus A$, the complement of $A$ in $\mathcal{U}$, which is the complement of $A$ as introduced in the preceding paragraph. With the sets $A$ and $B$ as in the previous example we have:

$$B \backslash A = \{4\};\ A \backslash B = \{-1, 0\}.$$

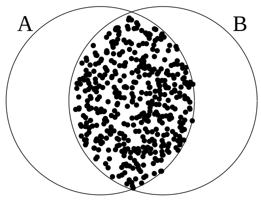
The use of the notation $A - B$ for difference is acceptable (becoming a little bit old-fashioned I think), but always bear in mind its true meaning: it has nothing to do with ordinary subtraction. Never be tempted to write $A + B$ when discussing sets as the plus sign is dangerous in this context.

Sets are often pictured as overlapping regions within one universal box and these drawings are called Venn[1] Diagrams. Those illustrating the ideas already introduced are pictured below:

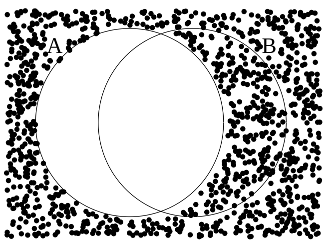
$A \cup B$



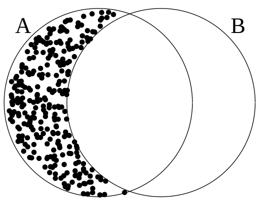

$A \cap B$




$\mathcal{U} \setminus A$




$A \setminus B$




[1]John Venn, 1834-1923, `http://www-history.mcs.st-and.ac.uk/history/Mathematicians/Venn.html`

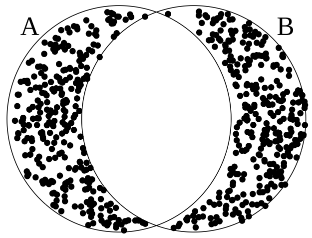
The idea of *exclusive or* (You may have a biscuit or a cake *but not both*!) can be expressed in the context of sets. The **symmetric difference** of two sets $A$ and $B$, denoted $A \triangle B$, consists of all elements contained in one of the sets $A$ and $B$ but not both:

$$A \triangle B = \{x : x \in A \text{or} x \in B \text{but not both}\}.$$

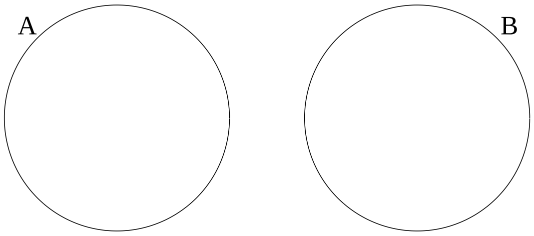
We now have the notation to express this more succinctly, it fact we can do this in two equivalent ways:

$$A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$$

$A \triangle B$




For the sets of Example 1.1 you should check that $A \triangle B = \{-1, 0, 4\}$.
Two sets $A$ and $B$ are **disjoint** if they have no elements in common: that is to say $A \cap B = \emptyset$.




If $A$ and $B$ are sets then an **ordered pair** from $A$ and $B$ (in that order) is a pair of elements $(a, b)$ where $a \in A$ and $b \in B$. The collection of all ordered pairs from $A$ and $B$ is known as the *direct product* or *cartesian product*[2] of $A$ and $B$. This set is denoted by $A \times B$. For example if $A = \{-1, 1, 3\}$ and $B = \{-1, 1\}$ then:

$$A \times B = \{(-1, -1), (-1, 1), (1, -1), (1, 1), (3, -1), (3, 1)\}.$$

The idea of an ordered pair you may have met before – in school mathematics or indeed in geography – the latitude and longitude of a point on the globe can be thought of as an ordered pair of numbers. The direct product is just the collection of all ordered pairs under consideration. The $\times$ notation does not of course mean 'multiply'. There is a connection with multiplication however through the cardinality of the set $A \times B$ which does equal $\#(A) \times \#(B)$: in the above example $\#(A) = 3, \#(B) = 2$ and the direct product $A \times B$ does indeed consist of $2 \times 3 = 6$ ordered pairs.

Note that an ordered pair may have a repeat (for example the pair $(1, 1)$ in the above example) and that, since order is an integral part of an ordered pair, the ordered pairs $(-1, 1)$ and $(1, -1)$ are different ordered pairs, although the sets $\{-1, 1\}$ and $\{1, -1\}$ are equal.

Version of 5.10.00

**Algebraic Laws of Sets**

[2]after René Descartes, 1596-1650, `http://www-history.mcs.st-and.ac.uk/history/Mathematicians/Descartes.html`

Sets obey the following laws. Let $A, B$ and $C$ denote arbitrary sets.

1. Idempotent Laws:
   1a: $A \cup A = A$   1b: $A \cap A = A$.
2. Associative Laws:
   2a $(A \cup B) \cup C = A \cup (B \cup C)$   2b $(A \cap B) \cap C = A \cap (B \cap C)$.
3. Commutative Laws:
   3a $A \cup B = B \cup A$   3b $A \cap B = B \cap A$.
4. Distributive Laws:
   4a $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$   4b $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

5 & 6. Identity Laws: if $\mathcal{U}$ is the universe, then
   5a $A \cup \emptyset = A$   5b $A \cap \mathcal{U} = A$
   6a $A \cup \mathcal{U} = \mathcal{U}$   6b $A \cap \emptyset = \emptyset$.

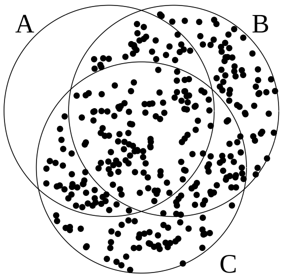
7. Involution Law: $(A^c)^c = A$ .

8 & 9. Complement Laws:
   8a $A \cup A^c = \mathcal{U}$   8b $A \cap A^c = \emptyset$
   9a $\mathcal{U}^c = \emptyset$   9b $\emptyset^c = \mathcal{U}$.

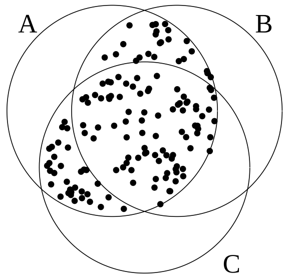
10. De Morgan's[3] Laws:
   10a $(A \cup B)^c = A^c \cap B^c$   10b $(A \cap B)^c = A^c \cup B^c$.

In order to convince oneself of a statement of equality of two sets it is often a good idea to represent the expressions involved by means of Venn Diagrams. For any algebraic expression involving at most three sets this is likely to be the fastest and safest method (for a human being). For instance, the distributive law 4b is easy to draw:

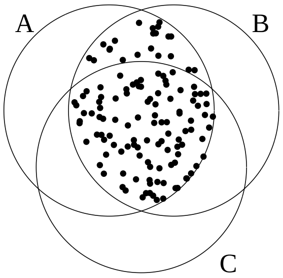
$B \cup C$



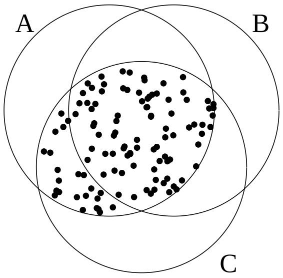

$A \cap (B \cup C)$



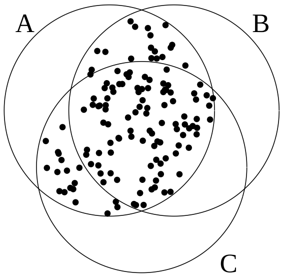

$A \cap B$




$A \cap C$




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




A second method, which is the one most pure mathematicians would try to use when the pictures get too complicated, is to find arguments (i) to show that any element of $X$ belongs to $Y$ (ii) to show that any

[3] Augustus de Morgan, 1806-1871, `http://www-groups.dcs.st-and.ac.uk/history/Mathematicians/De_Morgan.html`

element of $Y$ belongs to $X$. This can be very hard work, but let's see how it might be done in the case of the distributive law 4a:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \tag{1}$$

*First part* Take any $x \in A \cup (B \cap C)$. Then either $x \in A$ or $x \in B \cap C$. This gives us two cases to test. If $x \in A$ then $x \in A \cup B$ and $x \in A \cup C$ so that $x \in (A \cup B) \cap (A \cup C)$. If $x \in B \cap C$ then $x \in B$ and so $x \in A \cup B$; similarly $x \in A \cup C$. Hence $x \in (A \cup B) \cap (A \cup C)$ and so the LHS (left-hand side) of (1) is a subset of the RHS.

*Second part* Now suppose that $x \in (A \cup B) \cap (A \cup C)$. Then $x \in A \cup B$ and $x \in A \cup C$ which is the same as saying that $x \in A$ *or* $B$ and $x \in A$ *or* $C$. If $x \in A$ then certainly $x \in A \cup (B \cap C)$. Otherwise $x \notin A$ so $x \in B$ and $x \in C$; that is to say $x \in B \cap C$. Hence in either case, $x \in A \cup (B \cap C)$, and so the RHS of (1) is a subset of the LHS.

These two paragraphs together prove that equation (1) is always true for any sets $A, B$, and $C$. Since this is the case we say that (1) is an *identity*.

There is a definite symmetry about the ten Set Laws that is well worth appreciating. Let $E$ be an equation of set algebra. By the *dual equation* $E^*$ we mean the equation obtained form $E$ by replacing each occurrence of the symbols $\cup, \cap, \mathcal{U}, \emptyset$ by $\cap, \cup, \emptyset, \mathcal{U}$ respectively. Note that $(E^*)^* = E$: the dual statement of a dual statement is the original statement. Hence to say that $E^*$ is the dual of $E$ is equivalent to saying that $E$ is the dual of $E^*$: in language you will later become familiar with we say that duality is a symmetric relation. Law 7 is merely a statement about complements but all the other Laws occur in dual pairs. The upshot of this is that theorems about sets usually come in pairs.

**Principle of Duality** Let $E$ be a statement of inclusion or equality of sets involving only the operations of union, intersection and complementation. Then the statement $E^*$ obtained by interchanging unions with intersections, $\mathcal{U}$ with $\emptyset$, and reversing all inclusions is true if $E$ is true and is false if $E$ is false.

The reason why the Principle holds is that, given any proof of a statement $E$ we can turn it into a proof of $E^*$ by use of the dual Law at each stage: for example, if at one line in the proof we use Law 4a at the corresponding stage in the proof of $E^*$ we would use Law 4b.

The operations of union, intersection and complementation of sets are often referred to as *boolean*[4] *operations*. The question of deciding whether or not two boolean expressions represent the same set is in general extremely difficult, and is in fact one of the basic challenges of theoretical computing. When Venn diagrams and logical arguments both become too complicated, we can try to use the Set Laws to prove that an identity is true. For example:

**Example 2.1** Use the Set Laws to prove that:

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

and state the dual proposition.

**Proof**

$$\begin{aligned}
(A \cap B) \cup (B^c \cap A) &= (A \cap B) \cup (A \cap B^c) && \text{(by rule 3b)}\\
&= A \cap (B \cup B^c) && \text{(by rule 4b)}\\
&= A \cap \mathcal{U} && \text{(by rule 8a)}\\
&= A && \text{(by rule 5b).}
\end{aligned}$$

The dual proposition is

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

[4]George Boole, 1815-1864, `http://www-groups.dcs.st-andrews.ac.uk/history/Mathematicians/Boole.html`

Note how I gave, at every line of the argument, an exact reference to the Set Law I was using. You should think of this kind of proof as a printout of a computer program. If you really want to check that it's right, you need to verify each line in turn, and this is much easier if you're given the comment lines to tell you where to look up the thing you're checking at each point.

Version of 19.10.99

**The Counting Principle**

A set $A$ is *finite* if its cardinality $\#(A)$ is some natural number $n$; otherwise we say that $A$ is *infinite*. I ought to say what I mean by the natural numbers. I will use this opportunity to introduce three symbols for three infinite sets of numbers:

$\mathbb{N}$: the *natural numbers*: $\mathbb{N} = \{0, 1, 2, 3, \cdots\}$;[5]

$\mathbb{Z}$: the *integers*: $\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$;

$\mathbb{P}$: the *positive integers*: $\mathbb{P} = \mathbb{Z}^+ = \{1, 2, 3, \cdots\}$.

We next state and prove a simple but important fact that allows us to count the number of elements in a union of two finite sets $A$ and $B$.

**3.1 The Counting Principle** For finite sets $A$ and $B$:

$$\#(A \cup B) = \#(A) + \#(B) - \#(A \cap B)$$

For example, for the sets $A$ and $B$ of Example 1.1 of the first lecture one sees that $\#(A) = 4, \#(B) = 3, \#(A \cap B) = 2$ and $4 + 3 - 2 = 5$ which is indeed $\#(A \cup B)$.

It is easy to see why this works: $\#(A \cup B)$ will equal $\#(A) + \#(B)$ if and only if $A$ and $B$ are disjoint: otherwise the elements of $A \cap B$ will be counted twice in the sum $\#(A) + \#(B)$, and so the number $\#(A \cap B)$ can be viewed as a correction term to the initial rough guess of $\#(A) + \#(B)$. The formal proof below uses the idea, very common in counting problems, of partitioning the set to be counted into disjoint blocks and adding together the number of elements in each block. (Drawing a Venn Diagram of the sets involved will make things clear.)

**Proof of 3.1** We partition $A \cup B$ into 3 disjoint sets the union of which is $A \cup B$, namely $A \backslash (A \cap B), A \cap B$, and $B \backslash (A \cap B)$. Then

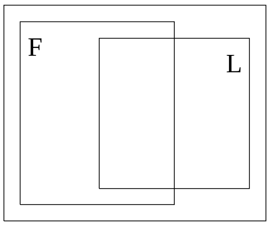
$$\begin{aligned} \#(A \cup B) &= \#(A \backslash (A \cap B)) + \#(B \backslash (A \cap B)) + \#(A \cap B) \\ &= (\#(A) - \#(A \cap B)) + (\#(B) - \#(A \cap B)) + \#(A \cap B) \\ &= \#(A) + \#(B) - \#(A \cap B). \end{aligned}$$

The Counting Principle can be applied repeatedly to yield a formula for $\#(A \cup B \cup C)$ and indeed a formula for the cardinality of a union of $n$ sets can likewise be developed. This general formula (the *Principle of Inclusion and Exclusion*) is very important in combinatorics and probability. It naturally involves quite a complicated expression. The pattern of the terms in the final formula is fairly easy to understand although it is somewhat more difficult to express accurately in words. I will content myself with going no further than the $n = 3$ case here to illustrate what I mean. The idea is to first treat $A \cup B \cup C$ as the union of two sets: $(A \cup B)$ and $C$ and apply the Counting Principle, following where it leads. To go from the first to the second line below we also make use of the Distributive Law to write $(A \cup B) \cap C$ as $(A \cap C) \cup (B \cap C)$.

[5] Mathematics is a living language. As with any human language, there are variations in dialect, and different mathematicians use symbols in different ways. Actually it's worse than most languages, because so many mathematicians are stiff-necked individualists! Specifically, while $\mathbb{Z}$ (or $Z$, or $\mathbf{Z}$) is pretty often used for the set of integers, you can never be sure whether $\mathbb{N}$ is going to contain 0 (which is the way I will use it in this course) or whether it's going to represent what I call $\mathbb{P}$. Any responsible author will of course take the trouble to explain exactly what s/he means by any symbol, which is what I'm doing here.

$$\begin{aligned}
\#((A \cup B) \cup C) &= \#(A \cup B) + \#(C) - \#((A \cup B) \cap C) \\
&= \#(A) + \#(B) - \#(A \cap B) + \#(C) - \#\big((A \cap C) \cup (B \cap C)\big) \\
&= \#(A) + \#(B) + \#(C) \\
&\qquad - \#(A \cap B) - \big(\#(A \cap C) + \#(B \cap C) - \#(A \cap B \cap C)\big) \\
&= \#(A) + \#(B) + \#(C) \\
&\qquad - \#(A \cap B) - \#(A \cap C) - \#(B \cap C) + \#(A \cap B \cap C).
\end{aligned}$$

**Example 3.2** In a school of 100 students, 50 take French, 40 take Latin and 20 take both languages. How many take no languages?




The required number is $\#((F \cup L)^c) = 100 - \#(F \cup L)$. Now, by the Counting Principle (for two sets)

$$\#(F \cup L) = \#(F) + \#(L) - \#(F \cap L) = 50 + 40 - 20 = 70.$$

Therefore the required number is 100 - 70 = 30.

**The Power Set**

**Definition 3.3** The *power set* $\mathcal{P}(A)$ of a set $A$ is the set of all subsets of $A$.

**Example 3.4** suppose that $A = \{a, b, c\}$; then

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{c, a\}, \{a, b, c\}\}.$$

In this case we have $\#(A) = 3$ and $\#(\mathcal{P}(A)) = 2^3 = 8$. This is a special case of the following important fact.

**Theorem 3.5** If $A$ is a finite set with $n$ members then $\#(\mathcal{P}(A)) = 2^n$.

**Remark:** This formula even holds when $A = \emptyset$ for $\mathcal{P}(\emptyset) = \{\emptyset\}$ and so we see that the power set of the empty set is not empty but has 1 element (that element being the empty set). This is in line with the formula as $2^0 = 1$.

**Proof of 3.5** One standard proof of this fact is to use a so-called inductive argument - a technique we shall learn later in the course. The following way of looking at the situation is perhaps the best however as it allows you to see more clearly what is going on.

List the elements of $A$ is some fixed order: $a_1, a_2, \cdots, a_n$ say. There is a one-to-one correspondence, a coding if you like, between subsets of $A$ (that is, members of $\mathcal{P}(A)$) and binary strings of length $n$, meaning strings of 0's and 1's of length $n$, established as follows. Let $(e_1, e_2, \cdots, e_n)$ be such a binary string (where each $e_i$ is either 0 or 1). The subset corresponding to this string contains the element $a_i$ if $e_i = 1$, but does not contain $a_i$ if $e_i = 0$. For example, if $A$ has elements $a_1, a_2, a_3, a_4$ in that order then the string (0 1 0 1) is a coding of the subset $\{a_2, a_4\}$.

Now, since there are two choices for each entry in a binary string of length $n$ and $n$ choices to make in all the total number of possible strings, and so the total number of subsets of $A$, is equal to

$$\underbrace{2 \times 2 \times \cdots \times 2}_{n\ times} = 2^n$$

This completes the proof.

Version of 5.10.00

## Relations

**Definition 4.1** Let $A$ and $B$ be sets. A *binary relation*, $R$, from $A$ to $B$ is a subset of $A \times B$. If $(x, y) \in R$ we say that $x$ is $R$-related to $y$ and write $x\ R\ y$. If $A = B$ then $R \subseteq A \times A$ and we say that $R$ is a *relation on* $A$.

**Examples 4.2** Take $A = B = \{1, 2, 3, 4\}$. The equality relation $=$ on $A$ is $\{(1, 1), (2, 2), (3, 3), (4, 4)\}$. The relation $<$ on $A$, where $a < b$ means $b - a$ is positive, is given explicitly as:

$$< \, = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}.$$

The *domain* $\mathrm{dom}(R)$ of a relation $R$ is the set of all first elements of the ordered pairs appearing in $R$; the *range* $\mathrm{ran}(R)$ of $R$ is the set of all second elements of the pairs. So, in the examples above,

$$\mathrm{dom}(=) = \{1, 2, 3, 4\}, \quad \mathrm{ran}(=) = \{1, 2, 3, 4\}.$$

$$\mathrm{dom}(<) = \{1, 2, 3\}, \quad \mathrm{ran}(<) = \{2, 3, 4\}.$$

Note: $\emptyset \subseteq A \times B; A \times B \subseteq A \times B$, so that both are relations from $A$ to $B$ known as the *empty* and the *universal* relation respectively.

## Representation of Relations

Most relations that we shall deal with will be between finite sets $A$ and $B$. Such relations can be represented by either

(i) a lozenge or arrow diagram;

(ii) an incidence matrix;

(iii) a directed graph (in the case where $A = B$).

We will explain these ideas by way of an example which itself involves an important type of relation on the integers.

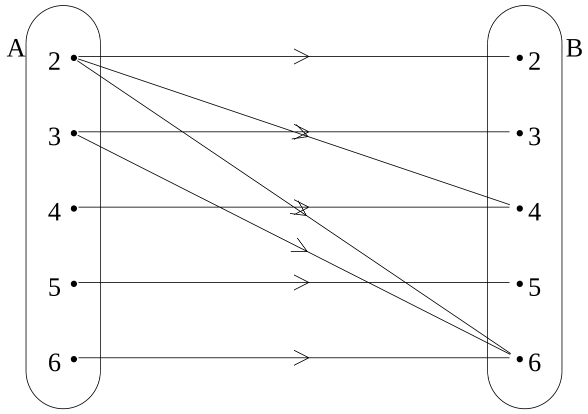
**Example 4.4** Let $A = B = \{2, 3, 4, 5, 6\}$.

**Notation:** For integers $a$ and $b$ write $a|b$, read '$a$ divides $b$', if $a \neq 0$ and $\frac{b}{a} \in \mathbb{Z}$. Note that '$a|b$' is the same as '$a$ is a factor of $b$' or '$b$ is a multiple of $a$'. Try not to confuse $a|b$ with $a/b$ ($a$ divided by $b$). For example $2|6$ is the *statement* that 2 is a factor of 6, while $2/6$ is a *number*, the rational number $1/3$ in fact.

Define a relation $R$ on $A$ as above by the rule that $a\ R\ b$ means that $a|b$. By inspection we see that:

$$R = \{(2, 2), (2, 4), (2, 6), (3, 3), (3, 6), (4, 4), (5, 5)(6, 6)\}.$$

The lozenge or arrow diagram of this relation $R$ then is as follows.

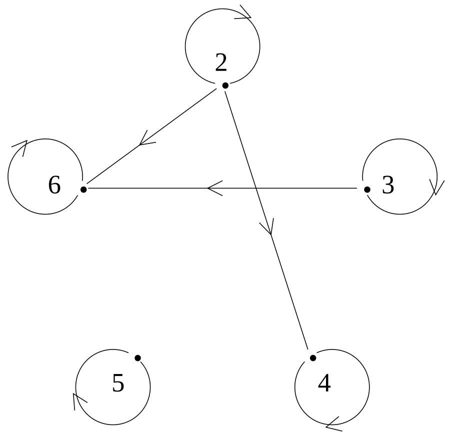



This kind of representation is useful when dealing with small relations – those not having too many pairs, and can be useful when explaining ideas involving relations as we shall see when we learn about the meaning of relation composition in the next lecture.

The *incidence matrix* $M_R$ of $R$ is a rectangular array of 0's and 1's with $\#(A)$ rows and $\#(B)$ columns. To specify this matrix we first need to agree on a fixed order for consideration of the members of $A$: $a_1, a_2, \cdots$ and the members of $B$: $\{b_1, b_2, \cdots\}$. The entry in the $i$th row and $j$th column of $M_R$ is a 1 if $a_i\ R\ b_j$ and is 0 otherwise.

$$M_R = \begin{array}{c} \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{ccccc} 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

When $A = B$ (as in the example here), the lozenge diagram can be simplified, in a way which is sometimes useful, by collapsing the two copies of the set $A = B$ together, so that only one point represents each of the elements of $A = B$, as follows:




This picture is called the *directed graph* or *digraph* of the relation $R$.

The **inverse** of a relation $R$ from $A$ to $B$, denoted by $R^{-1}$, is the relation from $B$ to $A$ (so that $R^{-1} \subseteq B \times A$) defined by:

$$R^{-1} = \{(b, a) : (a, b) \in R\}.$$

In other words we obtain $R^{-1}$ from $R$ by reversing the order of each pair in $R$. Taking $R$ to be the relation of Example 4.4 we get:

$$R^{-1} = \{(2, 2), (4, 2), (6, 2), (3, 3), (6, 3), (4, 4), (5, 5), (6, 6)\}.$$

In words: $b\ R^{-1}\ a$ if $b$ is a multiple of $a$.

Note that the digraph of $R^{-1}$ is the digraph of $R$ with all of the arcs reversed. The matrix $M_{R^{-1}} = M_R^T$, the *transpose* of $M_R$: that is the matrix obtained from $M_R$ by taking the $i$th row of $M_R$ (written from left to right) and transposing it into the $i$th column of $M_{R^{-1}}$ (written from top to bottom).

Version of 5.10.00

**Composition and Properties of Relations**

Let $R$ be a relation from $A$ to $B$, $S$ a relation from $B$ to $C$. We can form a new relation called the *composition* of $R$ and $S$ which is a relation from $A$ to $C$. This new relation is denoted by $R \circ S$ and is defined as follows:

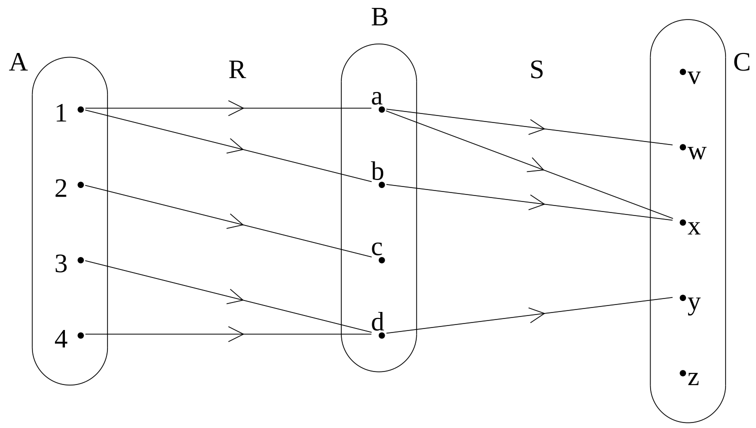
$$a(R \circ S)c \text{ if for some } b \in B,\ a\ R\ b \text{ and } b\ S\ c.$$

This definition may well leave you cold on a first reading (mathematical definitions often do), but an example may help clarify things.

**Example 5.1** Let $A = \{1, 2, 3, 4\}, B = \{a, b, c, d\}$, and $C = \{v, w, x, y, z\}$. Let $R$ and $S$ be the relations from $A$ to $B$ and from $B$ to $C$ respectively given by:

$$R = \{(1, a), (1, b), (2, c), (3, d), (4, d)\}, \ S = \{(a, w), (a, x), (b, x), (d, y)\}.$$

This is illustrated in the arrow diagram below.




The definition of $R \circ S$ means that a point in $a \in A$ is related to a point $c \in C$ if there is at least one path in the arrow diagram which begins at $a$ and ends at $c$, (necessarily passing through some point $b \in B$ on the way). For instance we see that $(1, x) \in R \circ S$ as there are in fact 2 such paths which start at 1 and finish at $x$: the first goes from 1 to $x$ via $a$, while the second goes from 1 to $x$ via $b$. On the other hand 2 is not a member of the domain of $R \circ S$ as there is no path from 2 into the set $C$ at all: from 2 we can only pass to $c \in B$ and $c$ does not lie in the domain of $S$ at all. Close inspection of the picture reveals that:

$$R \circ S = \{(1, w), (1, x), (3, y), (4, y)\}.$$

The arrow diagram does provide a nice mental picture to explain the meaning of $R \circ S$ but on the other hand if $R$ and $S$ involved many pairs these diagrams would be tedious to draw and would become a confusing mass of lines and arrows. The calculation can sometimes be kept more manageable through use of the incidence matrix approach. Let us write down the matrices for $R$, $S$, and $R \circ S$ and examine how the latter is obtained from the other two. We shall take the sets $A$, $B$ and $C$ to be listed in the order given above when working with the incidence matrices.

$$M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}, \quad M_S = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{ccccc} v & w & x & y & z \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

$$M_{R\circ S} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccccc} v & w & x & y & z \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

If you are familiar with how to multiply matrices together, the matrix for $M_{R\circ S}$ can be seen to be the usual product of matrices $M_R M_S$ *provided* that we convert any non-zero entry to 1; that is to say, we never count past 1. This is because we are only interested in the question as to whether there is a 'path' from $a \in A$ to $c \in C$, we are not interested in counting the number of such paths.

If you haven't seen 'ordinary' matrix multiplication before, the procedure is as follows. The matrix $M_{R\circ S}$ has the same number of rows as $M_R$ and the same number of columns as does $M_S$. To find the entry in, say, the *first* row and *third* column of $M_{R\circ S}$ we take the *first row* of $M_R$ and form the 'product' with the *third column* of $M_S$ as follows: we lay the row on top of the column, multiply corresponding entries and then sum these products: in this case the row concerned is (1 1 0 0) and the column (written horizontally for convenience) is (1 1 0 0). They both have to have four entries because there are four points in the set $B$. The entry in the first row and third column of $M_{R\circ S}$ is then:

$$1\cdot 1 + 1\cdot 1 + 0\cdot 0 + 0\cdot 0 = 1+1+0+0 \to 1$$

(The dots indicate multiplication.) This little calculation then corresponds to the fact that $(1, x) \in R \circ S$; the fact that $1 + 1$ occurs in the sum is due to the fact that there are not just 1 but 2 'paths' from 1 to $x$ in the arrow diagram, but remember, because we are only interested in whether or not there is a connection, we write 1 as the entry in $M_{R\circ S}$ rather than 2. You should work through the full multiplication of $M_R$ by $M_S$ and satisfy yourself that the answer given above is correct. In practice, when it comes to multiplying a row by a column you need only decide, when the row is superimposed on the column in question, does some 1 in the row meet some 1 in the column? If the answer is 'yes', then the corresponding entry in the product matrix is 1, otherwise it is 0.

In general, to find the entry in the $i$th row and the $j$th numbered column of $M_{R\circ S}$ we form the product, as described above, of the $i$th row of $M_R$ with the $j$th column of $M_S$.

**Theorem 5.2** Let $R$ be a relation from $A$ to $B$ and $S$ a relation from $B$ to $C$. Then $M_{R\circ S} = M_R M_S$, if we count any non-zero entry in $M_R M_S$ as 1.

The operation of adding incidence matrices has meaning too and we shall need to do just that in a few lectures' time. Let $R$ and $S$ be two relations from a set $A = \{a_1, a_2, \cdots, a_m\}$ to a set $B = \{b_1, b_2, \cdots, b_n\}$. To find the matrix of the relation $R \cup S$ we place a 1 at position $(i, j)$ if the pair $(a_i, b_j) \in R \cup S$; in other words the entry is 1 if and only if there is a 1 at position $(i, j)$ in one or both of the matrices $M_R$ and $M_S$. (This is similar to the way that matrices are ordinarily added together, except of course that since our matrices are binary we treat $1 + 1$ as 1.) In summary we have:

**Theorem 5.3** Let $R$ and $S$ be two relations from the set $A$ to the a set $B$. Then $M_{R\cup S} = M_R \vee M_S$.

**Properties of Relations**

Three important properties that a relation $R$ on a set $A$ may satisfy are the following:

1. $R$ may be *reflexive*: that is $a\ R\ a\ \forall a \in A$;
2. $R$ may be *symmetric*: if $a\ R\ b$ then $b\ R\ a$;
3. $R$ may be *transitive*: if $a\ R\ b$ and $b\ R\ c$ then $a\ R\ c$.

(I'm sorry. You just have to learn these words. There's as much sense to them as there is to most words in English. 'Transitive' means 'crossing over', for instance.)

**Definition 5.4** A relation $R$ on a set $A$ is said to be an *equivalence relation* (or sometimes just an *equivalence*) if $R$ is reflexive, symmetric, and transitive.

Before studying equivalences we give examples of relations which have two of the three properties above but lack the third, (the construction of an example of a symmetric and transitive relation which is not reflexive we shall defer till Lecture 6). This shows that the three properties above are *independent*, meaning that no two of them imply the third as a necessary consequence.

**Example 5.5** Let $A = \mathbb{Z}$, the set of integers. Define a relation $R$ by the rule that $a\ R\ b$ if $|a - b| \le 2$. (For those unfamiliar with the absolute value sign, that is the pair of vertical lines as it occurs in $|a - b|$, interpret this rule as saying that the distance between the two numbers $a$ and $b$ on the number line is no more than 2.)

Then $R$ is reflexive: $|a - a| = 0 \le 2$ and so $a\ R\ a\ \forall a \in \mathbb{Z}$;[6]

$R$ is symmetric: if $a\ R\ b$ then $|a - b| \le 2 \Leftrightarrow |b - a| \le 2$, which says that $b\ R\ a$.

However, $R$ is not transitive. To show this we need a counterexample: an instance in which the property fails. This is easily found in this case as $0\ R\ 2$ and $2\ R\ 3$ but $(0,3) \notin R$ as $|0 - 3| = 3 > 2$.

**Example 5.6** Let $A = \mathbb{P}$, the set of positive integers and define $R$ by the rule $a\ R\ b$ if $a|b$, that is, $a$ is a factor of $b$.

$R$ is reflexive as $a|a$ for every $a \in \mathbb{P}$ since $\frac{a}{a} = 1 \in \mathbb{Z}$;

$R$ is transitive: to see this, suppose that $a\ R\ b$ and $b\ R\ c$ for some $a, b, c \in \mathbb{P}$. Then there exist integers $r$ and $s$ such that $b = ar$ and $c = bs$. Substituting the first equation into the second gives $c = bs = (ar)s = a(rs)$, and since $rs \in \mathbb{P}$ this shows that $a|c$, which is to say that $a\ R\ c$, as required.

However $R$ is clearly not symmetric: for example $2\ R\ 4$ as $2|4$ but $4\ R\ 2$ is false as $4|2$ is false.

Version of 12.10.99

**Equivalence Relations**

In order to find an example of a relation on a set $A$ which is symmetric and transitive but not reflexive we need look no further than the empty relation! As long as $A$ is not itself empty, the empty relation is clearly not reflexive. It is however symmetric and transitive: both these properties say that *if* a certain pair, (or in the case of transitivity, certain pairs) are in $R$ then some other pair is also in $R$. If $R$ has no pairs at all therefore, these conditions are satisfied by default! Is it possible to find a less annoying example? Yes, but it is not altogether easy because of the following fact.

**Proposition 6.1** Suppose that $R$ is a symmetric and transitive relation on $A$ and that for each $a \in A$ there exists $b \in A$ such that $a\ R\ b$. Then $R$ is an equivalence relation.

**Proof** By the definition of equivalence relation, we need only check that in these circumstances $R$ is also reflexive. To see this, let $a \in A$. By hypothesis there is some $b \in A$ such that $a\ R\ b$. Since $R$ is symmetric we therefore have $b\ R\ a$ also. Since $R$ is transitive and $a\ R\ b$ and $b\ R\ a$, it follows that $a\ R\ a$. (Note that the definition of transitivity does not preclude the possibility that some of $a, b$ or $c$ in the definition are, as here, equal.) Since $a$ was an arbitrary member of $A$ we conclude that $R$ is reflexive, thus completing the proof.

Bearing this in mind, we present the following example of a relation which is symmetric and transitive but not reflexive.

**Example 6.1** Let $A = \mathbb{Z}$ and define $R$ by saying that $a\ R\ b$ if $ab > 0$.

$R$ is symmetric as $a\ R\ b$ means that $ab > 0 \Leftrightarrow ba > 0$, which is to say that $b\ R\ a$.

$R$ is transitive: suppose that $a\ R\ b$ and $b\ R\ c$ so that $ab > 0$ and $bc > 0$. Then multiplying these two inequalities together gives $ab^2c > 0$ whence $ac > 0$ (because $b^2 > 0$ as $b = 0$ is impossible since $ab > 0$). Hence $a\ R\ c$ and so $R$ is transitive.

However $R$ is *not* reflexive as $(0,0) \notin R$ as $(0,a) \notin R$ for all $a \in A$.

The idea of equivalence is the generalization of equality. The equality relation itself on a set is clearly an equivalence but very often two objects may be equivalent for your immediate purposes if they share a common property and indeed this is one typical source of equivalence relations. To take a simple-minded example, suppose you are interested in entering all the words in the English language and your concern for the moment is only with the number of characters in each word: that is to say that you consider two words equivalent if they have the same length; denote this relation by the symbol $\sim$ so that for instance `aardvark`

[6] I see that I have a new symbol here, $\forall$. This means 'for every' or 'for all'. So '$a\ R\ a\ \forall\ a{\in}\mathbb{Z}$' means '$a$ is related to itself for every integer $a$'.

$\sim$ `geometry` as both have 8 letters and so both take up the same space. It is very easy to see that $\sim$ is an equivalence relation on the set $A$ of all words. It is equally easy to see that $\sim$ breaks up the underlying set $A$ into disjoint blocks corresponding to word length, with every word residing in exactly one of these blocks or *equivalence classes* as they are generally called; for example the word `geometry` is a member of the block consisting of all 8-character words. This partitioning phenomenon of the underlying set $A$ by the equivalence relation is not peculiar to this example but is a feature of any equivalence relation on any set as we shall see shortly. Next we shall introduce a particularly important class of equivalences on the integers known as congruence modulo $n$.

**Example 6.2** Let $n$ be a fixed positive integer. Two integers, $a$ and $b$ are said to be *congruent modulo* $n$ if they differ by a multiple of $n$. This is written as $a \equiv b \pmod{n}$. There are several ways of formulating this definition:

$$a \equiv b \pmod{n} \Leftrightarrow n|(b-a) \Leftrightarrow b-a = kn \text{ for some } k \in \mathbb{Z} \Leftrightarrow b = a + kn$$

For example $13 \equiv 19 \pmod{3}$ as $19 - 13 = 6 = 2 \times 3$. Yet another way of looking at congruence mod $n$ is to say that $a \equiv b \pmod{n}$ if $a$ and $b$ leave the same remainder when divided by $n$: we see in this example that both 13 and 19 leave a remainder of 1 when divided by 3.

We shall verify that congruence modulo $n$ is an equivalence on $\mathbb{Z}$ shortly. First let us look at the case where $n = 2$. We see that we have:

$$\cdots \equiv -4 \equiv -2 \equiv 0 \equiv 2 \equiv 4 \equiv \cdots$$

$$\cdots \equiv -3 \equiv -1 \equiv 1 \equiv 3 \equiv \cdots$$

In other words two numbers are congruent modulo 2 if they are both even, or if they are both odd. In general equivalence modulo $n$ breaks the integers up into $n$ blocks. Two numbers $a$ and $b$ leave the same remainder $r$ say when divided by $n$ if and only if each has the form $kn + r$ (the values of $k$ will of course usually be different for $a$ and $b$). For the example of $13 \equiv 19 \pmod{3}$ we have $n = 3$ and $13 = 4 \times 3 + 1$ while $19 = 6 \times 3 + 1$. There are $n$ possible remainders when we divide by $n$ $(0, 1, 2, \cdots, n-1)$ and so that leads to $n$ equivalence classes modulo $n$. For example, for $n = 6$, the equivalence class of 0, which we shall denote by $[0]$, is given by $[0] = \{6k : k \in \mathbb{Z}\}$, the set of all integer multiples of 6. Another class is $[5] = \{6k + 5 : k \in \mathbb{Z}\}$. Note that $[-1] = [5]$ as $-1$ is of the required form $6k + 5$: $6k + 5 = -1$ *does* have an integer solution in $k = -1$.

The most common everyday situation where modular arithmetic arises is in the calculation of the day of the week. For example, if the Great Flood of Noah began on a Tuesday night when did it end? We all know that it rained for 40 days and 40 nights, that there are 7 days in a week, and that $40 \equiv 5 \pmod{7}$; 5 nights after Tuesday is Sunday, so it would have stopped raining on Sunday evening.

We now carefully verify that congruence modulo $n$ is an equivalence relation on $\mathbb{Z}$; $a, b, c$ denote arbitrary integers.

Reflexivity: $a \equiv a \pmod{n} \Leftrightarrow n|(a-a) \Leftrightarrow n|0$ which is true as $\frac{0}{n} = 0 \in \mathbb{Z}$.

Symmetry: suppose that $a \equiv b \pmod{n}$. This means that $\frac{b-a}{n} = k \in \mathbb{Z}$. But then $\frac{a-b}{n} = -k$, and since $-k \in \mathbb{Z}$ also we conclude that $b \equiv a \pmod{n}$.

Transitivity: suppose that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then $\frac{b-a}{n} = k$ say and $\frac{c-b}{n} = l$ say, where $k, l$ are integers. But then

$$\frac{c-a}{n} = \frac{c-b+b-a}{n} = \frac{c-b}{n} + \frac{b-a}{n} = l + k$$

and since $l + k$ is an integer also we conclude that $a \equiv c \pmod{n}$, as required in order to verify transitivity.

**Definition 6.3** Let $R$ be an equivalence relation on a set $A$ and let $a \in A$. The *equivalence class* of $a$ with respect to $R$, denoted by $[a]$ is

$$[a] = \{b \in A : a \; R \; b\}.$$

**Definition 6.4** A *partition* $P$ of a set $A$ is a collection of non-empty disjoint subsets of $A$ the union of which is the whole of $A$. That is to say the sets of $P$ cover $A$ and do not overlap each other.

**Theorem 6.5** The equivalence classes of an equivalence $R$ on a set $A$ form a partition of $A$.

**Proof** Since each element $a \in A$ is in the equivalence class $[a]$ (by reflexivity) it is clear that the equivalence classes of $R$ do cover the whole of $A$. The only thing which is not obvious is that equivalence classes are disjoint. Therefore we need to check that if two classes $[a]$ and $[b]$ share a common element, $c$ say, then in fact $[a] = [b]$. We shall verify that $[b] \subseteq [a]$; repetition of the argument with the roles of $a$ and $b$ interchanged would then yield the opposite inclusion $[a] \subseteq [b]$ thus giving the required conclusion $[a] = [b]$.

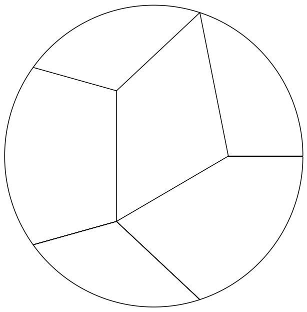
Since $c \in [a]$ we have $a\ R\ c$ and similarly $c \in [b]$ means that $b\ R\ c$. By symmetry, $b\ R\ c$ implies that $c\ R\ b$. We then have $a\ R\ c$ and $c\ R\ b$ and so by transitivity $a\ R\ b$ which is to say that $b \in [a]$. Now let $d \in [b]$ so that $b\ R\ d$. We then have $a\ R\ b$ and $b\ R\ d$ so again by transitivity $a\ R\ d$ and so $d \in [a]$. This shows that any member $d$ of $[b]$ lies in $[a]$ and so we have the desired conclusion that $[b] \subseteq [a]$.

In the next lecture we shall explore the exact relationship between equivalence relations and partitions.

Version of 5.10.00

**Partitions**

We have seen how every equivalence relation induces a partition of the underlying set $A$ into equivalence classes. Conversely given a partition of $A$ there is an equivalence relation which goes with it. A typical partition can be pictured as below.



The partition $P$ is the set of disjoint non-empty blocks which cover $A$. It is very natural to call two elements $a, b \in A$ equivalent, let us write $a \sim b$, if $a$ and $b$ lie in the same block. The three properties of reflexivity, symmetry and transitivity are immediately seen to be satisfied by the relation $\sim$ on $A$, and so $\sim$ is indeed an equivalence relation on $A$. What is more, the equivalence classes of $\sim$ are seen to be the blocks of the original partition $P$.

We saw in the last lecture that if we begin with an equivalence relation $R$ then the equivalence classes of $R$ form a partition $P$ of $A$. If we now take the equivalence relation $\sim$ induced by this partition $P$ as constructed in the preceding paragraph we see that $\sim$ and $R$ are the same. In conclusion we have a natural one-to-one correspondence between equivalence relations on a set $A$ and partitions of the set $A$. Equivalence relations and partitions can be viewed as two sides of the same coin.

**Partial Orders**

The idea of equivalence is the generalization of the notion of equality. The idea of partial order is the generalization of the relation $\leq$.

**Definition 7.1** A relation $R$ on a set $A$ is a *partial order* if $R$ is reflexive, transitive, and *anti-symmetric*. To say that $R$ is *anti-symmetric* means that:

$$a\ R\ b\ \&\ b\ R\ a \Rightarrow a = b$$

To get some feel of the meaning of partial order and in particular of the property of anti-symmetry think of the ordinary $\leq$ relation on any set of numbers; to be definite let us take the set to be $\mathbb{Z}$. It is impossible for $a \leq b$ and $b \leq a$ to be simultaneously true unless $a = b$.

The property of anti-symmetry is not too difficult to understand but it is different in nature to the others that we have met. Reflexivity says that certain pairs must be in $R$; symmetry and transitivity both say that if certain pairs are in $R$ then so are some other pairs. Anti-symmetry is different in that it effectively *forbids* certain pairs being in $R$ for anti-symmetry can be re-formulated as follows:

$$\textit{if } (a,b) \in R \textit{ then } (b,a) \notin R \textit{ unless } a = b.$$

A few things to note: first anti-symmetry *does not* imply reflexivity. Although the definition of anti-symmetry says that pairs of the form $(a,a)$ are not forbidden, it nowhere says that they *must* be included. (Mathematics is a free country. You don't have to do things just because they're allowed.) Second, anti-symmetry is not the same as being not symmetric as the next example illustrates.

**Example 7.2** Let $A = \mathbb{Z}$ and let $a\ R\ b$ if $a|b$. Then $R$ is not symmetric and $R$ is not anti-symmetric. $R$ is not symmetric because, for example, $(2,4) \in R$ but $(4,2) \notin R$. However $R$ is not anti-symmetric either as $(2,-2) \in R$ and $(-2,2) \in R$ yet $2 \neq -2$.

It is also possible for a relation $R$ to be both symmetric and anti-symmetric at the same time: for example the equality relation on any set $A$ has both properties. However, it is not difficult to show that a relation $R$ is symmetric and anti-symmetric if and only if $R$ is contained in the equality relation: that is to say $R$ only has pairs of the form $(a,a)$ and no others.

An example of a partial order is the usual $\leq$ relation on the integers where $a \leq b$ means that $b - a$ is a non-negative integer. We usually picture $a \leq b$ to mean that, on the number line, $a$ lies to the left of $b$ or $a = b$.

Once a relation $R$ is known to be a partial order it is often written using the symbol $\leq$. In this case we also write $a < b$ to mean that $a \leq b$ and $a \neq b$.

The one example of a partial order we have given so far is very special and enjoys many extra properties. In particular the standard ordering $\leq$ of the integers is an example of a total ordering. A partial order $\leq$ on a set $A$ is called *total* if, for any $a, b \in A$ either $a \leq b$ or $b \leq a$. This is just the case with the standard ordering $\leq$: any two numbers are *comparable*, meaning that either $a \leq b$ or $b \leq a$. A totally ordered set is sometimes also called a *linearly* ordered set or a *chain*. A total ordering is likewise sometimes described as a *linear ordering*. Are there any obvious examples of true partial orderings? partial orderings where some pair of elements of the underlying set are *incomparable*? We present two such examples now.

**Example 7.3** We take Example 7.2 except that instead of taking $A = \mathbb{Z}$ we restrict ourselves by taking $A = \mathbb{P}$, the set of positive integers. Then:

$R$ is reflexive as $a|a$ for all $a \in \mathbb{P}$ (it is critical here of course that $0 \notin \mathbb{P}$);

$R$ is transitive: suppose that $a|b$ and $b|c$. Then, as in Example 5.6, $a|c$.

$R$ is anti-symmetric: if $a|b$ and $b|a$, then, since $a$ and $b$ are both positive, it follows that $a = b$.

We conclude that $R$ is a partial order on $\mathbb{P}$ and what is more it is a true partial order in that many pairs of positive integers are incomparable: for instance neither $(5,14)$ nor $(14,5)$ lie in $R$, thus showing that $R$ is not total.

**Example 7.4** Let $S$ be any set and let $A = \mathcal{P}(S)$, the power set of $S$. For two subsets $X, Y$ of $S$ let us write $X \leq Y$ to mean that $X \subseteq Y$. It is an easy exercise to check that we are within our rights to write this relation using the symbol $\leq$ as it is a partial ordering of the subsets of $S$. (Indeed this is such a common way of partially ordering a collection of sets that this type of ordering is known as 'ordering by set inclusion'.) This ordering of $\mathcal{P}(S)$ is also not a total order as, provided $\#(S) \geq 2$, it is possible to find two subsets $X$ and $Y$ of $S$ which are incomparable with respect to this order in that $X \not\subseteq Y$ and $Y \not\subseteq X$.

As a particular instance of ordering by set inclusion consider $P$, the set of all relations on a set $A$. The members of $P$ are all the subsets of $A \times A$ and so the set $P$ can be ordered by set inclusion. Don't be frightened! All we are saying is that for two relations $R$ and $S$ on a set $A$ we write $R \leq S$ if every pair $(a,b) \in R$ is also a pair in $S$. Since there is a one-to-one correspondence between relations and their incidence matrices this partial ordering also gives a partial ordering of the incidence matrices of the relations on $A$: $M_R \leq M_S$ if and only if $R \leq S$. What does this amount to in terms of the matrices themselves? Answer:

> $M_R \leq M_S$ if whenever the entry in row $i$ and column $j$ of $M_R$ is a 1, then so is the entry in the same position in $M_S$.

This can be put in a slightly slicker if less transparent fashion. Let us write $m_{ij}$, $n_{ij}$ for the respective entries in the $i$th row and $j$th column of two $m \times m$ incidence matrices $M$ and $N$. ($m$ is the number of elements of $A$.) Then:

$$M \leq N \text{ if and only if } m_{ij} \leq n_{ij} \text{ whenever } 1 \leq i, j \leq m.$$

**Example 7.5** Let $A = \{a, b, c\}$ and

$$R = \{(a,a), (b,c)\}, \quad S = \{(a,a), (b,b), (b,c), (c,b)\}.$$

Then $R \leq S$ as $R \subseteq S$. Comparing incidence matrices we have:

$$M_R = \begin{array}{c c} & \begin{array}{ccc} a & b & c \end{array} \\ \begin{array}{c} a \\ b \\ c \end{array} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \end{array}, \quad M_S = \begin{array}{c c} & \begin{array}{ccc} a & b & c \end{array} \\ \begin{array}{c} a \\ b \\ c \end{array} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \end{array}$$

And we see that $M_R \leq M_S$ as every entry in $M_R$ is less than or equal to the corresponding entry in $M_S$: in other words, whenever we have a 1 in $M_R$ we find a 1 at the same position in $M_S$.

Version of 5.10.00

**Lexicographic Order**

Total orders are, as Winnie the Pooh said in a different context, comfortable sorts of things to have. In particular if we have a huge collection of strings of symbols, words if you like, it is best if they can be listed by some total ordering that is both easy to specify and use. Fortunately this problem was solved when they invented dictionaries, and it is this idea of alphabetical order that we next describe precisely.

We have a set $W$ of words over a totally ordered alphabet $A$. We construct a total order on $W$ as follows. Let $w_1, w_2$ be distinct members of $W$. We read the words $w_1, w_2$ from left to right and find the first place where they differ: let us suppose that it is the $i$th place so that the $i$th letter of $w_1$ is $a_i$ say, while that of $w_2$ is $b_i$. We now write $w_1 < w_2$ if $a_i < b_i$ in $A$ and if $b_i < a_i$ we write $w_2 < w_1$.

This rule makes sense if $w_1$ and $w_2$ are words of the same length, but not necessarily otherwise. We all know that in an ordinary dictionary `top` $<$ `topaz` but the rule as given does not deal with this situation. We can make the above rule make sense all the time if we introduce a blank symbol ␣ into our alphabet $A$ that is considered to come *before* all other letters of the alphabet. We now regard all words as before except that each is reckoned to be followed by an infinite string of blank symbols. This now makes all words the same length (the length is infinite, I realise, but often infinite things are more easily described than finite ones). Now the rule of the previous paragraph works all the time and we have a total order on $W$ known as the *lexicographic order* of $W$. For example comparing the words `top␣␣␣`$\cdots$ and `topaz␣␣`$\cdots$ we note that they first differ in the 4th place where `top␣␣␣`$\cdots$ has a ␣ while `topaz␣␣`$\cdots$ has an *a*; since ␣ $<$ `a` in our extended alphabet it follows that `top` $<$ `topaz` in the lexicographic ordering.

**Example 8.1** Let $A$ be the alphabet $\{*, ?, \alpha, \beta\}$ with order $\alpha < \beta < * < ?$. Order the following words lexicographically:

$$**, \quad *\alpha*?, \quad ?*, \quad \beta\alpha\beta, \quad \beta\beta, \quad ?*\alpha.$$

Solution:

$$\beta\alpha\beta < \beta\beta < *\alpha*? < ** < ?* < ?*\alpha.$$

**Functions**

The next fundamental concept I wish to introduce is that of *function*. Along with 'number' and 'set' this is one of the central ideas of mathematics, so important indeed that it has a life of its own, which cannot really be covered by any formal definition. So perhaps I should start with some examples. For instance:

everyone has a mother (and only one). So we have a function 'mother-of', defined on the set of all people, where we say that 'mother-of($p$)' is the mother of $p$, it being understood that $p$ here must be a person.

A more familiar function (at least to mathematicians) is the function '$x^2$': if $x$ is any real number, then we can calculate the value of $x^2 = x \times x$. In the course here, the most important function we've yet seen is $\#$, the counting function: if $A$ is a set, then $\#(A)$ is the number of elements of $A$.

Now let me try to say what are the common features of all these operations (mother-of, squaring, counting) which mathematicians in the last hundred years have come to focus on.

(i) For any function, there is a well-defined set (the **domain** of the function) of objects to which the function can be applied.

(Thus the domain of the mother-of function is the set of all people; the domain of the real squaring function is the set of all real numbers; the domain of the counting function is the class of all finite sets.)

(ii) For each object in the domain of the function, there is exactly one thing which is the 'value' of the function at that object.

Something I want to emphasize here is that we may or may not have any way of *calculating* the function. The functions built into your calculators, like $x^2$ or $\sqrt{x}$, do correspond to strict rules for working out what the values are. But a function like 'mother-of' doesn't have such a rule. I am perfectly sure that everyone here has, or had, exactly one (biological) mother. That doesn't mean at all that I can work out who anybody's mother was. Similarly, I know that the set $E$ of earwigs in this room is finite; but I've got no effective way of deciding what $\#(E)$ is.

The next thing I want to say is that you must get into the habit of specifying the domain of a function before you try to do anything with it. The function 'mother-of' can I suppose be applied to animals (and even plants) as well as people. But you don't expect it to behave in the same way if you make such an extension, and it's better practice to say right at the start what objects you are going to apply the idea to. In the C programming language, when you introduce a name for a function, you are required to say whether it will be applied to integers or to floating-point numbers or whatever; the same discipline is necessary everywhere in mathematics if you're going to keep out of trouble.

It is also important (though, some of the time, less absolutely vital) to watch out for the sort of values your function takes. Thus my function 'mother-of' always takes people as its values (provided, at least, that it's applied to people); the squaring function (when applied to real numbers) takes real values; and the counting function (when applied to finite sets) takes non-negative integer values. In order to help us keep track of these things a standard notation has grown up which I want you to learn and stick to faithfully. The phrase

$$f : A \to B$$

means that

$f$ is a function;

$A = \operatorname{dom} f$ is the domain of $f$, that is, the set of objects to which the function is going to be applied;

$B$ is a set such that the value $f(x)$ of $f$ at the object $x$ belongs to $B$ for every $x \in A$.

Note that there's a fundamental asymmetry in this formula. *Every* point $x$ of $A$ corresponds to (exactly one) value $f(x)$ of the function $f$. *Every* value $f(x)$ of $f$ belongs to $B$. But there may be points of $B$ which get missed by the function. (For instance: if we define $f : \mathbb{N} \to \mathbb{N}$ by saying that $f(n) = n + 1$ for $n \in \mathbb{N}$, then 0 is not a value of $f$.)

By the rule I have just given, the domain of a function $f : A \to B$ is the whole set $A$. The **range** or **set of values** of $f$ is

$$\operatorname{ran} f = \{b \in B : \text{there is some } a \in A \text{ such that } b = f(a)\},$$

and in general there is no reason why $\operatorname{ran} f$ should be the whole of $B$. For that reason we have a separate word for the set $B$; it is called a *codomain* of the function $f$.

**Composition of Functions**

From the point of view of abstract set theory almost the most important thing you can do with two functions is to *compose* them, that is, apply one and then the other.

**Definition 8.2** Let $f : A \to B$ and $g : B \to C$ be functions. Then we have a function $g \circ f : A \to C$ defined by saying that $\mathrm{dom}(g \circ f) = A$ and $(g \circ f)(x) = g(f(x))$ for every $x \in A$; this is the **composition** of the functions $g$ and $f$.

**Remember!** In $g \circ f$, $f$ acts first and $g$ acts second.

(I rather hope that you resent having to remember that functions compose backwards. Mathematicians are sometimes very inconsiderate in things like this. But this time there is actually a reason for it. This is because we have a golden rule

$$(g \circ f)(x) = g(f(x)).$$

In this formula, the brackets move around a bit, and the little circle turns up on the left, but $g$, $f$ and $x$ stay in the same order. This will make it *much* easier to handle things like $h \circ (g \circ f)$, when we come to them.)

**Example** Find the rules which describe the composite functions $g \circ f$ and $f \circ g$, where $f$ and $g$ are both functions from $\mathbb{Z}$ to itself and $f(n) = 2n - 1$, $g(n) = n^2$ for every $n \in \mathbb{Z}$.

Since in this case the sets $A$, $B$ and $C$ of our general definition are all equal to $\mathbb{Z}$, we can compose the two functions in either order. First:

$$(g \circ f)(n) = g(f(n)) = g(2n - 1) = (2n - 1)^2;$$

$$(f \circ g)(n) = f(g(n)) = f(n^2) = 2n^2 - 1$$

Hence we have $(g \circ f)(n) = (2n - 1)^2$ and $(f \circ g)(n) = 2n^2 - 1$.

Are $g \circ f$ and $f \circ g$ the same? Well, the formulae $(2n - 1)^2$ and $2n^2 - 1$ *look* different, so probably $g \circ f \neq f \circ g$. But 'probably' isn't really good enough in mathematics. You might think that the formulae $(1 + 2 + \ldots + n)^2$ and $1^3 + 2^3 + \ldots + n^3$ looked different; but when you come to work them out they always give the same answers. So let's check. The first thing to do is to look at a couple of special values – starting with the easy ones! For instance,

$$(g \circ f)(1) = (2 \times 1 - 1)^2 = (2 - 1)^2 = (-1)^2 = 1,$$

$$(f \circ g)(1) = 2 \times 1^2 - 1 = 2 \times 1 - 1 = 2 - 1 = 1$$

(eh?) These came out the same. So we really do have to ask: have we got the same function twice, or was it just an accident? Try another:

$$(g \circ f)(0) = (2 \times 0 - 1)^2 = (0 - 1)^2 = (-1)^2 = 1,$$

$$(f \circ g)(0) = 2 \times 0^2 - 1 = 2 \times 0 - 1 = 0 - 1 = -1.$$

So *here* the two functions give different answers, and they must be different functions.

Generally speaking, changing the order in a function composition will rarely give the same result as before.

### Injective and surjective functions

Functions come in a bewildering variety of types. Of course I am not going to try to give you a full list of the things which mathematicians have found interesting and important about functions. But just as, when studying relations, we find that 'symmetric' and 'transitive' relations are particularly worth studying, there are two kinds of function which I should like to describe straight away.

**Definition 8.3** A function $f : A \to B$ is called *one-to-one* or **injective** if for each $b \in B$ there is *at most* one $a \in A$ such that $f(a) = b$. Another way of saying the same thing is to say that

$$\text{for any } a_1, a_2 \in A,\ f(a_1) = f(a_2) \Rightarrow a_1 = a_2,$$

or

$$\text{for any } b \in B, \text{ the equation } f(x) = b \text{ has at most one solution.}$$

**Definition 8.4** A function $f : A \to B$ is *onto* or **surjective** if $\mathrm{ran}\, f = B$, that is, for any $b \in B$, the equation $f(x) = b$ has at least one solution.

Putting these two ideas together, we have the idea

**Definition 8.5** A function $f : A \to B$ is called **bijective** if $f$ is both surjective and injective, that is,

for any $b \in B$, the equation $f(x) = b$ has exactly one solution.

The properties of injectivity and surjectivity are preserved by function composition.

**Theorem 8.5** Let $f : A \to B$ and $g : B \to C$ be two functions. If $f$ and $g$ are both injective then so is $g \circ f$. If $f$ and $g$ are both surjective then so is $g \circ f$.

**Proof:** Suppose that $f$ and $g$ are both one-to-one. Consider $g \circ f : A \to C$ and suppose that $a_1$, $a_2$ are distinct members of $A$. Then $f(a_1) \neq f(a_2)$, because $f$ is injective. But now $g(f(a_1)) \neq g(f(a_2))$ because $g$ is injective. So

$$(g \circ f)(a_1) = g(f(a_1)) \neq g(f(a_2)) = (g \circ f)(a_2),$$

and $(g \circ f)(a_1) \neq (g \circ f)(a_2)$. And this works whenever $a_1$ and $a_2$ are distinct members of $A$, so $g \circ f$ is injective.

Next suppose that $f$ and $g$ are both surjective. We need to prove that $g \circ f$ is surjective, that is to say that $\text{ran}(g \circ f) = C$. To prove this we must take an arbitrary element $c \in C$ and show that there is some $a \in A$ such that $(g \circ f)(a) = c$. Now, since $g$ is surjective there is some $b \in B$ such that $g(b) = c$. Similarly, since $f$ is surjective there is some $a \in A$ such that $f(a) = b$. This element $a \in A$ then has the required property, because

$$(g \circ f)(a) = g(f(a)) = g(b) = c$$

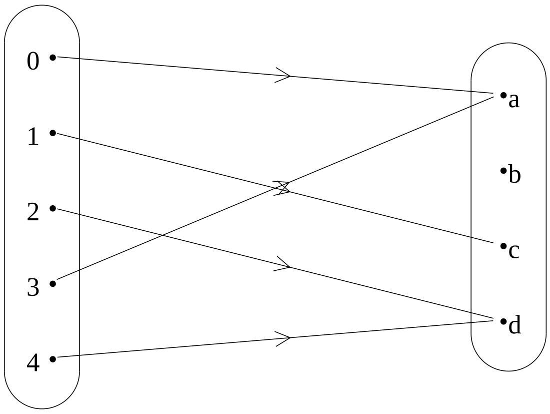
as required.

**Corollary 8.6** Let $f : A \to B$ and $g : B \to C$ be bijections. Then $g \circ f : A \to C$ is also a bijection.

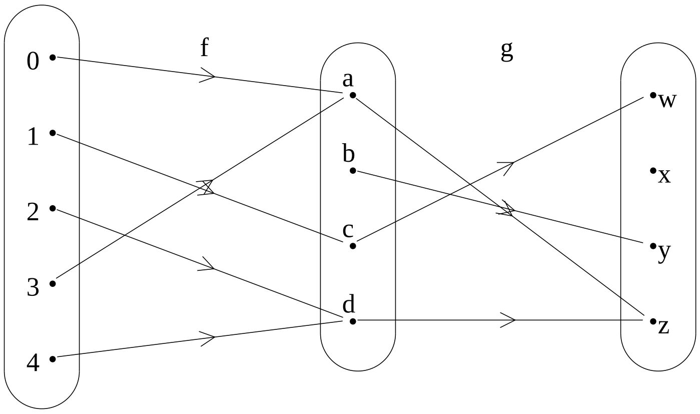
**Proof:** This follows immediately from the previous theorem and the definition of bijection. In detail: because $f$ and $g$ are both bijections, they are both injections, so $g \circ f$ is an injection; because $f$ and $g$ are both bijections, they are both surjections, so $g \circ f$ is a surjection; thus $g \circ f$ is both an injection and a surjection, and must be a bijection.

**Inversion of functions** After 'composition', the next generally important idea to sort out is that of 'inversion'. Suppose that $f$ is an injection; write $A$ for its domain and $B$ for its set of values. Then $f : A \to B$ is a bijection. So for any $b \in B$ there is exactly one $a \in A$ such that $f(a) = b$. This means that we can define a function $f^{-1} : B \to A$ by the rule: for any $b \in B$, $f^{-1}(b)$ is to be that member of $A$ which is mapped onto $b$ by the function $f$; that is, $f^{-1}(b) = a$ iff $f(a) = b$.

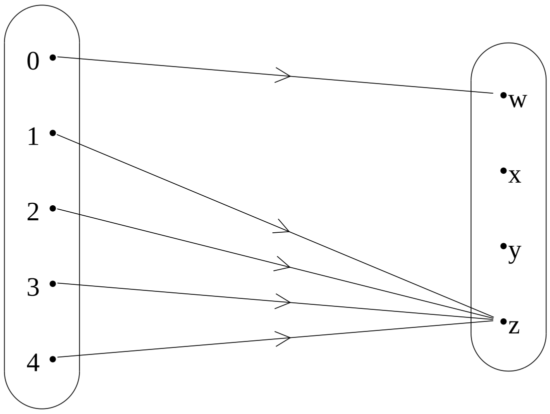
**Arrow diagrams of functions** Just as we can sometimes get a better idea of what a relation (between small finite sets) looks like by drawing its arrow diagram, we can do the same for functions. Suppose we have a function $f : \{0, 1, 2, 3, 4\} \to \{a, b, c, d\}$ defined by saying that $f(0) = a$, $f(1) = c$, $f(2) = d$, $f(3) = a$ and $f(4) = d$. Then the arrow diagram looks like




If we want to look at the composition of this with another function, we can put the arrow diagrams together. Suppose we have $g : \{a, b, c, d\} \to \{w, x, y, z\}$ defined by setting $g(a) = g(d) = z$, $g(b) = y$ and $g(c) = w$, the picture looks like

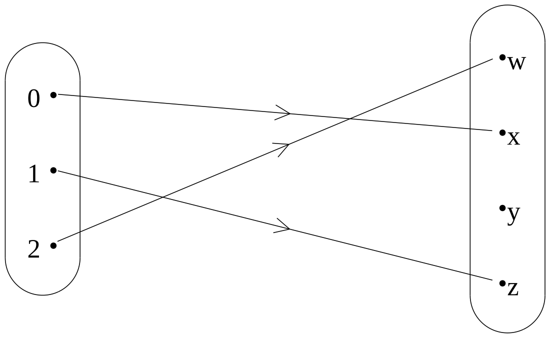



From this we can read off the composition $g \circ f$; we have $(g \circ f)(0) = (g \circ f)(2) = (g \circ f)(3) = (g \circ f)(4) = z$ and $(g \circ f)(1) = w$, with arrow diagram

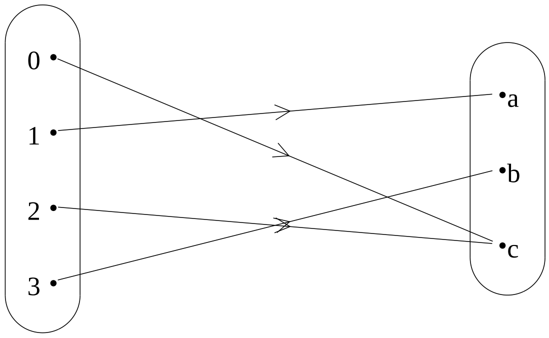



If you have the diagram in front of you, you should be able to see at once whether your function is injective or surjective or both or neither. For instance, looking at the picture for $f$ above, we see that there are arrows running from both 0 and 3 to $a$, that is, $f(0) = f(3) = a$; but this means that $f$ takes the value $a$ twice, and cannot be injective. Similarly, $g(a) = g(d) = z$ so $g$ isn't injective. As for surjectivity, there's no arrow running to $b$ in the diagram for $f$, that is, $b \in B \setminus \operatorname{ran} f$, and $f$ (regarded as a function from $\{0, 1, 2, 3, 4\}$ to $\{a, b, c, d\}$) isn't surjective.

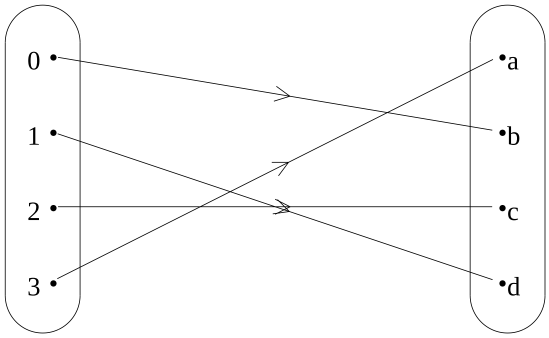
A typical injective function looks like this:



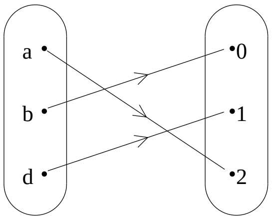

with at most one arrow arriving at each point on the right-hand side. A typical surjective function looks like

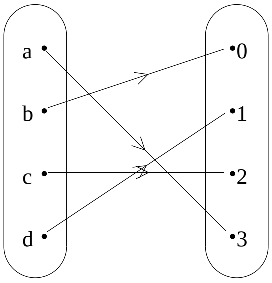


with at least one arrow arriving at each point on the right; while a bijective function looks like




with exactly one arrow reaching each point on the right. The first and third have inverses, which are




Note that in the first of these the point $c$ got left out of the domain of the inverse function because it wasn't in the set-of-values of the original function.

**Relations and functions** Of course the arrow diagrams here will remind you of the arrow diagrams we drew for relations. If you look at the arrow diagrams I have drawn in the last few pages, you will I hope notice that they share a striking property: from every point in the left-hand set, there is always exactly one arrow. This is the difference between a function and other kinds of relation. Look again at the first function I drew, in which $f(0) = f(3) = a$, $f(1) = c$ and $f(2) = d$. If we forget that this is supposed to be a picture of a function, and interpret it instead as the diagram of a relation, the relation is the set $R = \{(0, a), (1, c), (2, d), (3, a), (4, d)\}$. This is called the **graph** of the function; generally, for any function $f$, its graph is the set $\Gamma = \{(x, f(x)) : x \in \operatorname{dom} f\}$ of all the pairs $(x, y)$ in which $x$ belongs to the domain of the function and $y = f(x)$ is the value of the function at that point.

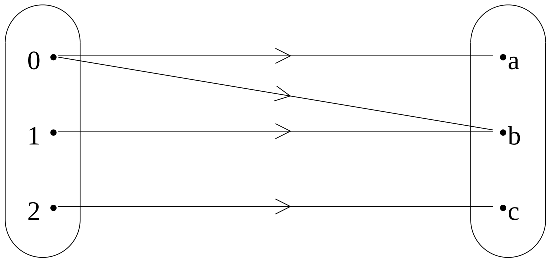
Now if you know the set $\Gamma$, you can work out what the function must have been, by saying that

$$\operatorname{dom} f = \{x : \text{there is some } y \text{ such that } (x, y) \in \Gamma\}$$

(indeed, this is what I earlier called the domain of the relation $\Gamma$), and

$$\text{for any } x \in \operatorname{dom} f,\ f(x) \text{ is that } y \text{ such that } (x, y) \in \Gamma.$$

This process won't, of course, work on all relations. If we have the relation

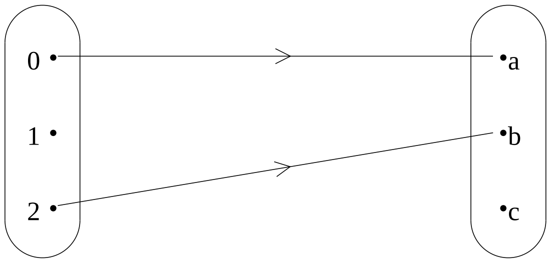



then there's no problem in deciding what the domain is (it's $\{0,1,2\}$), but when we come to ask what $f(0)$ ought to be we have two rival candidates $a$ and $b$, and no way to decide between them; so this relation is not the graph of a function. A relation $R$ will be the graph of a function if, and only if,

$$\text{for every } x \text{ there is at most one } y \text{ such that } (x,y) \in R.$$

This is sometimes called the **unicity property**.

Even when a relation $R$ has the unicity property, we still have to watch out for the domain of the corresponding function. If, for instance, $R$ is the relation




then the domain of the corresponding function $f$ is $\{0,2\}$, not $\{0,1,2\}$; $f(0)=a$, $f(2)=b$ but no value is assigned to $f(1)$. So when we have a relation $R$ between $A$ and $B$, and want to know whether it can be regarded as a function from $A$ to $B$, we have to check not only unicity but also **totality**: $R \subseteq A \times B$ has the totality property if $A = \operatorname{dom} R$, that is, for every $a \in A$ there is a $b \in B$ such that $(a,b) \in R$.

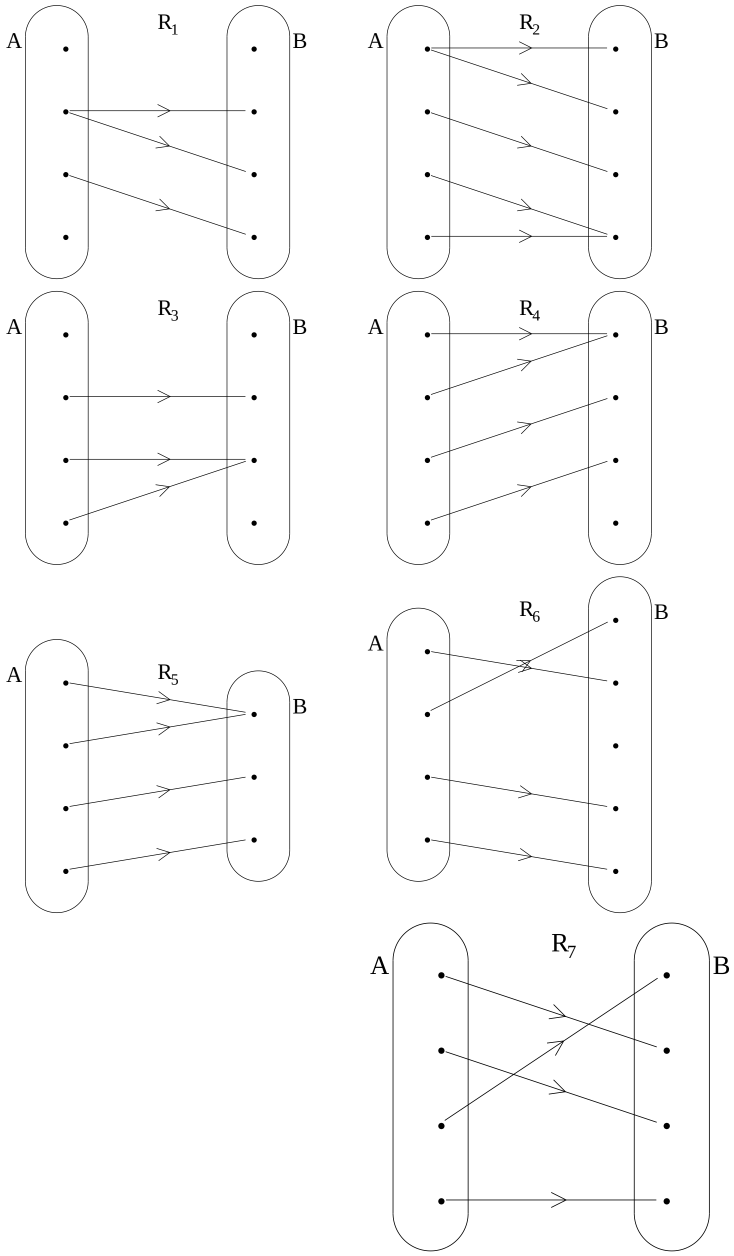
If we associate relations and functions in this way, we find that (for an injective function $f$) the graph of its inverse function $f^{-1}$ is just the inverse $\Gamma^{-1}$ of the graph $\Gamma$ of $f$. (All this is saying is that

$$f^{-1}(y) = x \iff f(x) = y \iff (x,y) \in \Gamma \iff (y,x) \in \Gamma^{-1}.)$$

But a **warning!**: *compositions come out the wrong way round.* If $f : A \to B$ and $g : B \to C$ are functions, with graphs $\Gamma_f \subseteq A \times B$ and $\Gamma_g \subseteq B \times C$, then the graph of the composition $g \circ f$ is

$$\begin{aligned}
\Gamma_{g\circ f} &= \{(x, g(f(x)) : x \in A\} \\
&= \{(x,z) : z = g(f(x))\} \\
&= \{(x,z) : \text{ there is some } y \text{ such that } f(x) = y \text{ and } g(y) = z\} \\
&= \{(x,z) : \text{ there is some } y \text{ such that } (x,y) \in \Gamma_f \text{ and } (y,z) \in \Gamma_g\} \\
&= \Gamma_f \circ \Gamma_g,
\end{aligned}$$

not $\Gamma_g \circ \Gamma_f$. Sorry!




To give you practice, I have drawn the arrow diagrams of seven relations to show the different things which can happen.

1. $R_1$ is a relation which is not a function, because it lacks 'unicity'; with the set $A$ as drawn, it also lacks 'totality'.

2. $R_2$ is a relation which is not a function, because it lacks 'unicity'; but with the set $A$ as drawn, it has 'totality'.

3. $R_3$ is a function, that is, a relation which has 'unicity'; but with the set $A$ as drawn, it does not have 'totality', that is, its domain is not the whole set $A$. We cannot therefore say that '$R_3$ is a function from $A$ to $B$'.

4. $R_4$ is a function from $A$ to $B$, but it is neither injective nor surjective.

5. $R_5$ is a function from $A$ to $B$; it is surjective but not injective.

6. $R_6$ is a function from $A$ to $B$; it is injective but not surjective. The inverse relation $R_6^{-1}$ is a function, but the domain of $R_6^{-1}$ is not the whole of $B$.

7. $R_7$ is a bijective function from $A$ to $B$; its inverse is a bijective function from $B$ to $A$.

It is a useful exercise to write down the incidence matrices of these seven relations and observe how the special properties involved manifest themselves in the matrix representation. You should observe the following:

a. $R$ has 'totality' (as for $R_2$ and $R_4$-$R_7$) iff each row of $M_R$ contains at least one 1.

b. $R$ has 'unicity' (as for $R_3$-$R_7$) iff each row of $M_R$ has no more than one 1.

c. $R$ is a function with domain $A$ (as for $R_4$-$R_7$) iff each row of $M_R$ has exactly one 1.

d. If $R$ is a function, then it is surjective iff each column of $M_R$ has at least one 1.

e. If $R$ is a function, then it is injective iff each column of $M_R$ has at most one 1.

f. $R$ is a bijection from $A$ to $B$ iff each row and each column of $M_R$ has exactly one 1. (In this case $M_R$ must be a *square* matrix, meaning that it has the same number of rows as columns.)

Version of 6.10.00

If $f$ and $g$ are two injective functions, then we find that the composition $f \circ g$ is also injective. To see this, suppose that we know that $(f \circ g)(x_1) = (f \circ g)(x_2)$. Then $f(g(x_1)) = f(g(x_2))$. But $f$ is injective, so this can happen only when $g(x_1) = g(x_2)$; and since $g$ is also injective, $x_1$ must be equal to $x_2$. Thus the only way in which $(f \circ g)(x_1)$ can be equal to $(f \circ g)(x_2)$ is when $x_1 = x_2$, which is what we mean by saying that $f \circ g$ is injective.

This means that $f \circ g$, like $f$ and $g$, has an inverse. We also have a formula for $(f \circ g)^{-1}$ which is a bit like the formula for the inverse of compositions of relations: if $f$ and $g$ are injective functions, then $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$. This is because

$$\begin{aligned}
&x = (f \circ g)^{-1}(y) \\
&\quad \Longleftrightarrow y = (f \circ g)(x) \\
&\quad \Longleftrightarrow y = f(g(x)) \\
&\quad \Longleftrightarrow f^{-1}(y) = g(x) \\
&\quad \Longleftrightarrow g^{-1}(f^{-1}(y)) = x \\
&\quad \Longleftrightarrow (g^{-1} \circ f^{-1})(y) = x.
\end{aligned}$$

**The inverse of the composition is the composition of the inverses *backwards*.**

**Drawing graphs** When we have 'real' functions, that is, functions such that both the domain and the set of values are subsets of the real line $\mathbb{R}$, then we can draw the function by drawing its graph. For instance, if $f$ is the function defined by saying

$$\operatorname{dom} f = \mathbb{R}, \quad f(x) = x^2 \text{ for every } x \in \mathbb{R},$$

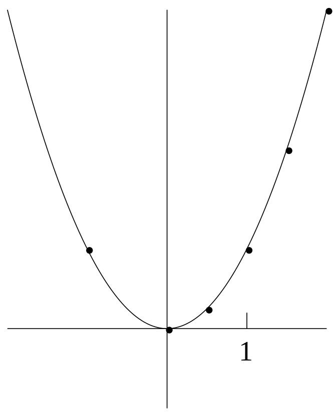
then the graph of $f$ is the set

$$\Gamma_f = \{(x, f(x)) : x \in \operatorname{dom} f\} = \{(x, x^2) : x \in \mathbb{R}\} = \{(x, y) : x \in \mathbb{R},\ y \in \mathbb{R},\ y = x^2\},$$

and we can draw this as the set of points

$$(0,0), (1,1), (-1,1), (2,4), (\tfrac{1}{2}, \tfrac{1}{4}), (1\tfrac{1}{2}, 2\tfrac{1}{4}), \dots\},$$

which, joined up, make a nice smooth curve.



This is an effective way of getting an mental picture of the differences between different functions – but it works well only for these rather special functions in which both $x$ and $f(x)$ are real numbers; for the most interesting functions to a computer scientist, it's not often much help.

**The $\mapsto$ notation** I said above that when looking at a function we must as soon as possible decide what its domain is. As long as we are in any doubt whatever about this, we haven't understood what we're doing. But it is sometimes useful to start with a notion of the 'action' (e.g., 'squaring' or 'counting') before getting down to the details of where we're going to apply it. So we sometimes write

$$x \mapsto x^2$$

to refer to the idea of 'squaring' before settling on a domain. I repeat that this formula by itself doesn't define a function, because it doesn't tell us what the domain is. But if I write

$$n \mapsto n^2 : \mathbb{Z} \to \mathbb{N}$$

then this is a reasonable shorthand for 'the function $f$, with domain $\mathbb{Z}$, such that $f(n) = n^2$ for every integer $n$'.

For example, let $A$ be the set of all linear equations with integer coefficients:

$$A = \{\text{`}mx + n = 0\text{'}: m,\, n \in \mathbb{Z}\}.$$

If we wish to talk about this set extensively (and especially, if we were writing a computer package to manipulate equations of this type) we should soon notice that a particular member of $A$ is specified once the ordered pair $(m, n)$ is specified. Just for the sake of abbreviation therefore we would be led to consideration of the bijection $f : \mathbb{Z} \times \mathbb{Z} \to A$ defined by saying that $f(m,n)$ is the equation '$mx + n = 0$', that is, the bijection $(m,n) \mapsto$'$mx + n = 0$': $\mathbb{Z} \times \mathbb{Z} \to A$. What this is doing is 'coding' equations in terms of a couple of parameters. This idea is very simple: you should not try to read too much into it. However, the mathematicians among you especially may have got into the habit of expecting that functions would map numbers onto other numbers. To be happy with functions like the one above which maps equations to ordered pairs of integers requires a certain flexibility of mind, but nothing more.

Version of 15.10.99

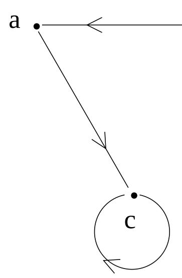
### Transitive Closure of a Relation

As you know, some relations are transitive and some aren't. But for any relation $R$, there's an associated transitive relation, the **transitive closure** $R^*$ of $R$, which is the smallest transitive relation on which includes $R$. That's a rather abstract way of putting it. But if you think about any relation which actually matters, its transitive closure is likely to be important too. For instance, most people care about their descendants, and many people care about their ancestors. Who are your ancestors? They're your parents, and the parents of your parents, and the parents of the parents of your parents, and .... Starting from the relation $R$, where $x\,R\,y$ if $x$ is the parent of $y$, we move to the relation $R^*$, where $x\,R^*\,y$ if there is some chain $x$, $a$, $b, \ldots, y$, starting at $x$ (the ancestor) and finishing at $y$ (the descendant) with $x\,R\,a$, $a$, $R$, $b$, $b\,R\,c$

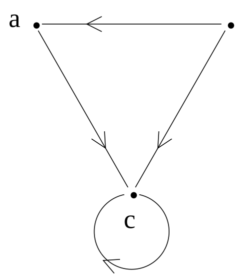
and so on, finishing with $p\,R\,y$ after finitely many steps. You can do this for any non-transitive relation; for instance, if you have the relation '$x\,S\,y$ if $x$ knows $y$', then we shall have $x\,S^*\,y$ if $x$ knows someone who knows someone who knows someone who knows someone who ... knows someone who knows $y$.

There's no reason, indeed, why you shouldn't start from a *transitive* relation. If $R$ is transitive, you just get $R^* = R$, so nothing new has happened. But if you don't know whether $R$ is transitive or not, then you can still go through the process of building its transitive closure.

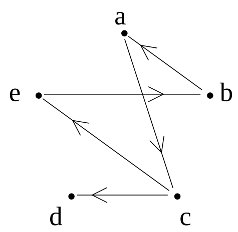
If a relation is small enough for us to be able to draw its digraph, we can expect to be able to draw the digraph of its transitive closure without much trouble. Let me give an example. Suppose the relation is $\{(a,c),(b,a),(c,c)\}$, so that its digraph is



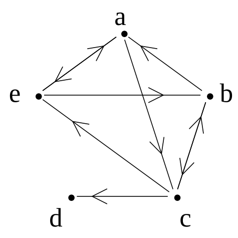

On this diagram, look for 'paths', that is, chains $p \to q \to r \ldots$ in which you have arrows going from one point to the next. (In the diagram here, we have such a path $b \to a \to c$.) Now put in shortcuts. The point is that if we have a chain $p \to q \to r$ in the diagram, then $p\,R\,q$ and $q\,R\,r$, so we shall have to have $p\,R^*\,r$, and we need to draw the arrow $p \to r$. In the diagram here, we have a path $b \to a \to c$, so we add the arrow $b \to c$:



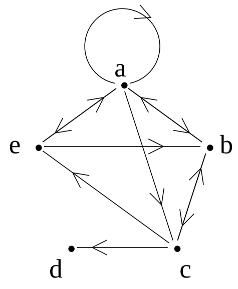

The problem is knowing when to stop! But you just have to be systematic. You must keep adding arrows until the diagram is transitive, and you can check transitivity by going over it point-by-point; is there a path through $a$ without the shortcut drawn in? is there a path through $b$ without the shortcut drawn in? is there a path through $c$ without the shortcut drawn in? For a more elaborate example, let's try



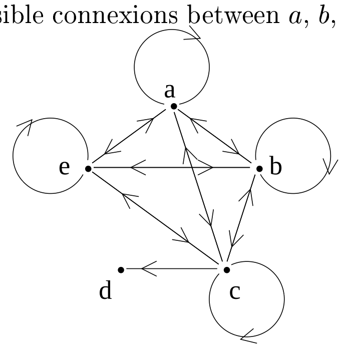

Here we can see rather a lot of paths needing shortcuts, e.g., $a \to c \to e$ and $c \to e \to b$ and $e \to b \to a$ and $b \to a \to c$. So put in the arrows $a \to e$, $c \to b$, $e \to a$, $b \to c$:



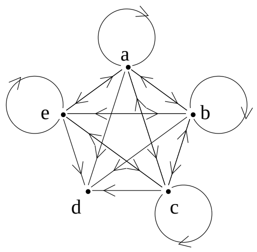

We now have paths $a \to e \to b$, so we had better put in a path $a \to b$. But also notice that we have paths $a \to e \to a$, that is, we know that $a\,R^* e$ and $e\,R^* a$, so we shall also have $a\,R^*\,a$, and we must add a loop at $a$:




Carrying on in this way, we get all possible connexions between $a$, $b$, $c$ and $e$, including a loop at each point:




So far I've left $d$ out on a limb. But since we have $a \to c \to d$ we'll have to have $a \to d$, and similarly for the others:




Here finally we have a transitive relation, and can stop. Notice the way in which the *cycle* $a \to c \to e \to b \to a$ in the original diagram led to the *complete graph* on the four vertices $a$, $b$, $c$, $e$ in the last two pictures.

For computers, of course, this is not a suitable method, and there are reasonably efficient algorithms for calculating the incidence matrix of the transitive closure from the incidence matrix of a relation; but I pass these by for now. It is however worth looking for a moment at reflexivity, symmetry and transitivity in terms of incidence matrices. Suppose that $R$ is a relation on a set $A$ with incidence matrix $M_R$.

**Reflexivity** $(a, a) \in R$ for all $a \in A$ – this corresponds to the leading diagonal of $M_R$ (that is the diagonal from top left to bottom right of the matrix) consisting entirely of 1's.

**Symmetry** $(a, b) \in R$ if and only if $(b, a) \in R$ – this corresponds to the entry with co-ordinates $(i, j)$ (that is the entry in the $i$th row and $j$th column) being always the same as the entry in position $(j, i)$. Now observe that when one takes the transpose of a matrix the effect is exactly to swap the entry at $(i, j)$ with that of $(j, i)$. If $R$ is symmetric, we have just observed that that will make no difference. In other words:

$$R \text{ is symmetric if and only if } M_R = M_R^T.$$

Matrices which equal their own transpose are themselves called *symmetric*.

**Anti-symmetry**: $R$ is anti-symmetric means that if $(a, b) \in R$ then $(b, a) \notin R$ unless $a = b$. In terms of $M_R$ this amounts to saying that if $i \neq j$ then $(i, j)$ is $1 \Rightarrow (j, i)$ is 0.

**Transitivity** This a little harder. Recall that $R$ is transitive iff

$$a \; R \; b \; \& \; b \; R \; c \Rightarrow a \; R \; c.$$

Now consider the composite relation of $R$ with itself: $R \circ R$. By the definition of relational composition, a pair $(a, c)$ will lie in $R \circ R$ exactly when there exists $b \in A$ such that $a \, R \, b$ and $b \, R \, c$. The relation $R$ will be transitive therefore if and only if all the pairs $(a, c)$ of $R \circ R$ already lie in $R$. That is, $R$ is transitive if and only if $R \circ R \subseteq R$. Recall that, with respect to this order, we have for any two relations $R$ and $S$ on $A$, $R \subseteq S$ if and only if $M_R \leq M_S$. In particular $R$ is transitive means exactly that $M_{R \circ R} \leq M_R$. Finally, since $M_{R \circ S} = M_R M_S$ we have $M_{R \circ R} = M_R^2$, and so we have proved the following result.

**Theorem 10.1** A relation $R$ on a set $A$ is transitive if and only if $M_R^2 \leq M_R$.

Version of 5.10.00

### Countable and Uncountable Sets

So far we have divided sets into two types - finite and infinite. However, as we shall see, not all infinite sets are of the same 'size'. This may sound surprising: at first sight it may seem natural to claim that it is nonsense to suggest that one infinite set is larger than another. However we can make sense of the idea if we look at things in the right way.

The first to draw attention to the peculiarities of infinite sets was Galileo[7]. What he noted was that sets such as $\mathbb{P}$, the positive integers, can be put into one-to-one correspondence with proper subsets of themselves. To be precise he noted that the function $f : \mathbb{P} \to \mathbb{P}$ where $f(n) = 2n$ is a bijection of the positive integers onto the even positive integers, leaving the odd integers out of the range. In one sense, the sets $\mathbb{P}$, $E$ (the evens) and $O$ (the odds) are of the same size as it is possible to find a bijection from any one of these sets to any other. On the other hand $E$ is a proper subset of $\mathbb{P}$ and so is in another sense smaller. There is nothing to worry about in this, except to note that finite sets never behave this way – if we take a proper subset $A$ of a finite set $B$ then it is always the case that $\#(A) < \#(B)$ and it is not possible to find a surjective function $f : A \to B$.

Having noticed that two infinite sets which you would have thought were different sizes can be matched together by some bijection, most people would give up; it looks as though we just have to put up with infinite sets being peculiar, and there doesn't seem to be anything more to say. But (what doesn't seem to have been noticed for more than two hundred years after Galileo) there are, in fact, infinite sets which *can't* be matched by any bijection; what is more, these infinite sets are in no way exotic, but are sets which have been studied (at least) since the time of Eudoxus.[8] Some infinite sets can be written in a list, and some cannot. This will be the focus of our attention in the rest of the next two lectures.

The set of positive integers can be listed in a sequence in the obvious way: $1, 2, 3, \cdots$: indeed this set embodies the very idea of an infinite list. However, some other infinite sets can be put into one-to-one correspondence with the positive integers and so be listed as well. For instance take the set $\mathbb{Z}$ of all integers:

$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}.$$

[7] Galileo Galilei, 1564-1642; `http://www-history.mcs.st-and.ac.uk/history/Mathematicians/Galileo.html`

[8] Eudoxus of Cnidos, 408-355 B.C.; `http://www-history.mcs.st-and.ac.uk/history/Mathematicians/Eudoxus.html`

This set comes to us naturally as a kind of doubly infinite list. It can however be rearranged into a list with a starting point as follows:

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, 4, -4, \cdots\}$$

In fact we shall make use of the idea used here more than once: if we have two lists:

$$a_1, a_2, a_3, \cdots, \ b_1, b_2, b_3, \cdots$$

we can interleave them to form a single list:

$$a_1, \ b_1, \ a_2, \ b_2, \ a_3, \ b_3, \cdots$$

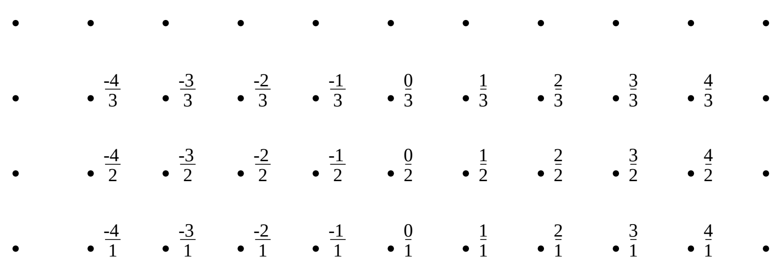
This is really what we did to combine the positive and negative whole numbers into a single list. You may think there is nothing much going on here. Given any set surely it is possible to consider it as a list in some way? But how about the set $\mathbb{Q}$ of all rational numbers?

The rational numbers can be regarded as the set of all fractions, positive, negative and 0, cancelled to lowest terms. The integers are considered to be a subset of $\mathbb{Q}$.

In fact $\mathbb{Q}$ can be written in a list. (If you are concerned by exactly what is meant by 'writing an infinite list', put your worries aside for the time being – I will try to clarify this a little later.)

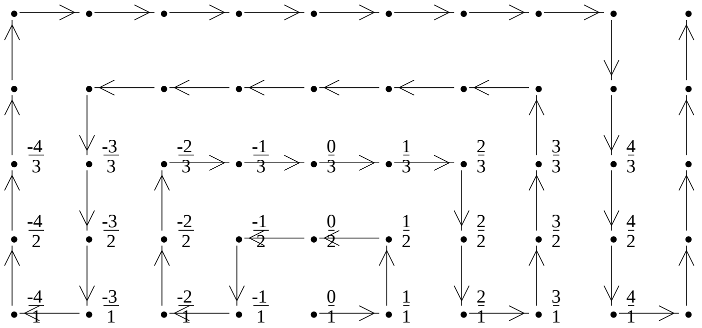
This looks a tough job as the rationals are *dense* in the sense that between any two of them, there is another one. So it looks as though we're going to start missing some out from the very beginning. This however causes no real trouble as long as we do not insist that we write our numbers in any particular order. We can always come back to one we've missed out. What we have to do is work out some systematic way of writing a list down which will eventually catch every rational number, both positive and negative. Actually there are lots of ways of doing it; every mathematician has his own favourite. Here's mine. First I'd better repeat what the set $\mathbb{Q}$ is: it's the set of all fractions $\frac{m}{n}$ where $m \in \mathbb{Z}$ (that is, $m$ is an integer, either positive or negative) and $n \in \mathbb{P}$ (that is, $n$ is a positive integer, not allowing 0). Now this is how *I* do it:

Start by drawing a picture, *not* of the set $\mathbb{Q}$, but with enough points so that I can label them with rational numbers in such a way that every rational number turns up at least once, like this:




What I have done here is to label the point with horizontal coordinate $m$ and vertical coordinate $n$ with the rational number $\dfrac{m}{n}$; I am using all integers $m$, but only strictly positive integers $n$, of course.

Trace a path through the diagram, calling at every point:



I started at $\frac{0}{1}$ and went back-and-forth; but you can go any way you like as long as you visit every point eventually.

Read off the numbers in the order in which you come to them:

$$\frac{0}{1}\quad\frac{1}{1}\quad\frac{1}{2}\quad\frac{0}{2}\quad\frac{-1}{2}\quad\frac{-1}{1}\quad\frac{-2}{1}\quad\frac{-2}{2}\quad\frac{-2}{3}\quad\frac{-1}{3}\quad\frac{0}{3}\quad\frac{1}{3}\quad\frac{2}{3}$$
$$\frac{2}{2}\quad\frac{2}{1}\quad\frac{3}{1}\quad\frac{3}{2}\quad\frac{3}{3}\quad\dots$$

Rewrite the fractions in lowest terms, so that you can spot the duplicates:

$$0\quad 1\quad \tfrac{1}{2}\quad 0\quad -\tfrac{1}{2}\quad -1\quad -2\quad -1\quad -\tfrac{2}{3}\quad -\tfrac{1}{3}\quad 0\quad \tfrac{1}{3}\quad \tfrac{2}{3}$$
$$1\quad 2\quad 3\quad \tfrac{3}{2}\quad 1\quad \dots$$

Now go through the list again without the duplicates:

$$0\quad 1\quad \tfrac{1}{2}\quad -\tfrac{1}{2}\quad -1\quad -2\quad -\tfrac{2}{3}\quad -\tfrac{1}{3}\quad \tfrac{1}{3}\quad \tfrac{2}{3}$$
$$2\quad 3\quad \tfrac{3}{2}\quad \dots$$

so that we have a list – an infinite list, of course – in which every rational number appears exactly once.

I hope that some of you are actually thinking about how to write a computer algorithm to print out a list of rationals. If you do, you should notice very quickly that the process I've proposed is jolly inefficient. But I learnt long ago that one should never try to write a fast program until one's got a slow one up, running and debugged.

Before we go any further I will try to make the idea of 'listing' more precise. What does it mean to have an infinite set $A = \{a_1, a_2, \cdots, a_n, \cdots\}$ given as a list? To answer this, write $a_1$ as $f(1)$, similarly put $f(2) = a_2$ and generally let us put $f(n) = a_n$. What we then have is a function $f : \mathbb{P} \to A$, but not just any function. The elements $a_n$ should exhaust all the elements of $A$ – no member of $A$ should miss out, for otherwise the list would only be a partial list of some of the members of $A$ and not others. In other words the function $f$ above is a surjective function – its range is the whole of $A$ and not just some subset. Finally, we are not interested in listing any member of $A$ more than once so we see that $f$ is injective also: if $m \neq n$ then $f(m) \neq f(n)$. This leads to the following definition.

**Definition 11.1** An infinite set $A$ is called **denumerable** if there exists a bijection $f : \mathbb{P} \to A$. A set $A$ is called **countable** if $A$ is finite or if $A$ is denumerable. Otherwise $A$ is called **uncountable**.

So the arguments above are supposed to show how to build bijections from $\mathbb{P}$ to $\mathbb{Z}$ and from $\mathbb{P}$ to $\mathbb{Q}$, so that $\mathbb{Z}$ and $\mathbb{Q}$ are denumerable (therefore countable). For instance, the list I gave of the rational numbers can be interpreted as the table of a function $f : \mathbb{P} \to \mathbb{Q}$ defined by setting

$$f(1)=0,\ f(2)=1, f(3)=\tfrac{1}{2},\ f(4)=-\tfrac{1}{2},\ f(5)=-1,\ f(6)=-2,\ f(7)=-\tfrac{2}{3},$$
$$f(8)=-\tfrac{1}{3},\ f(9)=\tfrac{1}{3},\ f(10)=\tfrac{2}{3},\ f(11)=2,$$
$$f(12)=3,\ f(13)=\tfrac{3}{2},\ f(14)=\ldots$$

and because every rational number appears exactly once on the list, $f$ is a bijection from $\mathbb{P}$ to $\mathbb{Q}$; $\mathbb{Q}$ is denumerable.

The question remains though: are there any uncountable sets? It turns out that the set of all real numbers $\mathbb{R}$ is uncountable. For our purposes a real numbers is any one which can be written as a decimal expansion. Any rational number is real – in fact the rationals are exactly those numbers which have recurring decimal expansions (this includes terminating decimals, of course). 'Most' real numbers do not have recurring patterns: $\sqrt{2}$ and $\pi$ are examples, although we shall not pause to prove that here. We are faced now with a real difficulty. How can we possibly be sure that it is impossible to write a particular set in the form of an infinite list? Just because we cannot see any way of doing it proves nothing. After all, you might not have been able to find a bijection from $\mathbb{P}$ to $\mathbb{Q}$ by yourselves, but that doesn't mean that there isn't one.

Version of 5.10.00

**Which sets are countable?**

We shall show that there is no way of listing all real numbers between 0 and 1. This astonishing fact was discovered by Cantor[9]. It is based on the observation, to be explained more carefully in a moment, that given any infinite list $L$ of decimals between 0 and 1 it is possible to use the list itself to construct another decimal between 0 and 1 that does not lie in the original list $L$. It follows immediately from this that there is no list $L$ which contains every real number between 0 and 1.

**Theorem 12.1** Let $f : \mathbb{P} \to [0,1]$ be any function.[10] Then there is a number $a \in [0,1]$ which is not a value of $f$.

**proof** Express each value of $f$ as a decimal:

$$\begin{aligned}
f(1) &= 0.a_{11}a_{12}a_{13}a_{14}\ldots\\
f(2) &= 0.a_{21}a_{22}a_{23}a_{24}\ldots\\
f(3) &= 0.a_{31}a_{32}a_{33}a_{34}\ldots\\
f(4) &= 0.a_{41}a_{42}a_{43}a_{44}\ldots\\
&\ldots\\
f(n) &= 0.a_{n1}a_{n2}a_{n3}a_{n4}\ldots\\
&\ldots
\end{aligned}$$

(A couple of points to watch here. Some numbers have got more than one decimal expansion; for instance, $0.200000\ldots = 0.199999\ldots$. In these cases it doesn't matter which you use. Next, if $f(k)=1$ then to put it in the form above we need to take the expansion $1 = 0.999999\ldots$.) Now build a new number as follows:

if $a_{11}=1$, set $a_1=2$; otherwise, set $a_1=1$;
if $a_{22}=1$, set $a_2=2$; otherwise, set $a_2=1$;
if $a_{33}=1$, set $a_3=2$; otherwise, set $a_3=1$;
if $a_{44}=1$, set $a_4=2$; otherwise, set $a_4=1$;
if $a_{55}=1$, set $a_5=2$; otherwise, set $a_5=1$;

[9] Georg Cantor, 1845-1918; `http://www-history.mcs.st-and.ac.uk/history/Mathematicians/Cantor.html;http://www.math.csusb.edu/history/public_html/HistTopics/Beginnings_of_set_theory.html#5`.

[10] I don't think I've used this [, ] notation before. $[0,1]$ is just the set of real numbers between 0 and 1, including 0 and 1 themselves.

and so on. At the end, look at the number

$$a = 0.a_1a_2a_3a_4\ldots.$$

Now $a \neq f(1)$, because $a_1 \neq a_{11}$; $a \neq f(2)$, because $a_2 \neq a_{22}$; $a \neq f(3)$, because $a_3 \neq a_{33}$; and, generally, $a \neq f(n)$ because $a_n \neq a_{nn}$.

Thus we have built a real number $a$, between 0 and 1, which is not a value of the function $f$.

**Notes on the argument** Cantor's argument has always been found very difficult. It has been attacked on various philosophical grounds which we needn't go into. From our point of view, the important problem is to make sense of it at all. It's very abstract with some horrid formulae in it. I don't think there's any way round this. For look at what the theorem says:

'for any function $f : \mathbb{P} \to [0, 1]$, there's a number $a$ which isn't a value of $f$'.

Now the whole point of this is that the function comes first. What the theorem says is that if *you* have a function from $\mathbb{P}$ to $[0, 1]$, then *I* can find a number which isn't a value of your function. You have to move first, by saying what function you are thinking of, before I have to say which number you didn't catch. (After all, if I told you which my favourite number was, you could take it for $f(1)$, and catch it at once.) So if I'm going to persuade you that I can win *every* time, and not just when you've been a little careless in picking your function, I've got to display a strategy, a general rule I can use whatever function you come up with. And there's no obligation on you to pick a function with a pretty formula for it. Look at the function I built in the last lecture, setting up a bijection from $\mathbb{P}$ to $\mathbb{Q}$. You would have every right to use something quite as awful as that.

You see also that I can't 'finish' the construction of the number $a$ in finitely many operations. But this stands to reason; I can't possibly complete my move without looking at everything your function does, and that will take infinitely long. But I did give you a recipe for $a$ which means that I can tell you the first 7 decimal coefficients of $a$ as soon as you've told me the first 7 decimal coefficients of each of the numbers $f(1), \ldots, f(7)$; so that if you have an effective method of actually calculating your function, I can come back with an equally effective method of calculating $a$.

The general principle of treating a mathematical statement as a theorem about a *game* ('If the first player chooses a function, the second player can find a number it doesn't catch') is a very useful way of handling the logic of many problems in pure mathematics.

**Corollary 12.2** $[0, 1]$ is not countable.

(For 12.1 tells us that there is no surjection from $\mathbb{P}$ onto $[0, 1]$, so surely there can be no bijection; and $[0, 1]$ is obviously[11] infinite.)

What all this is supposed to do is to show that we have three kinds of set:

finite sets,

countable sets which aren't finite, that is, 'denumerable' sets,

uncountable sets, that is, infinite sets which aren't denumerable;

and the point of 12.1-12.2 is to show that one of the basic sets of mathematics, the 'unit interval' $[0, 1]$, is an uncountable set, so that not only are there uncountable sets, but that any extensive use of set theory in mathematics is likely to run into them.

Now when Cantor came up with this in 1874 it was a revolutionary insight, and in fact we are still discovering new ways in which uncountable sets can be extraordinary. But in the present course we can get by with some fairly simple notions. The basic idea is that 'small' sets are countable and 'large' sets aren't. (There are actually important ways in which uncountable sets differ more from denumerable sets than denumerable sets differ from finite sets.) To make sense of this idea of 'small' and 'large' we need a basic fact:

**Proposition 12.3** If $A$ is a subset of $B$, then
(a) if $B$ is countable, so is $A$;
(b) if $A$ is uncountable, so is $B$.

[11] Whenever a mathematician says 'obviously', you should ask yourself (i) could *I* explain this to a five-year-old, and how would I do it (ii) could *s/he* explain it to a five-year-old?

(Can you see that these are saying exactly the same thing?) For suppose $B$ is countable. If $A$ is finite, we can stop. If $A$ is infinite, then surely[12] $B$ is also infinite; but it is countable, so there must be a bijection $f : \mathbb{P} \to B$, that is, a listing of $B$ as $b_1$ $(= f(1))$, $b_2$, $b_3, \dots$. Work along this list from the beginning. As soon as you come to a member of $A$, pull it out and call it $a_1$; when you come to the next member of $A$, call it $a_2$; and keep going. Because every member of $B$ is somewhere in the list, and $A \subseteq B$, you'll catch every member of $A$ sooner or later, so getting a listing of $A$ as $\{a_1, a_2, a_3, \dots\}$, that is, a bijection from $\mathbb{P}$ to $A$. So $A$ is countable.

In the argument above, I had to make an uncomfortable move when I realized that of course $A$ could be finite, in which case there won't be a bijection from $\mathbb{P}$ to $A$. This didn't matter at all, because (on the rules laid down in the last lecture) finite sets are countable. But it will be a nuisance to have to keep talking about finite sets separately, so it will be helpful to have a lemma[13] at this point.

**Lemma 12.4** (a) If $A$ and $B$ are two sets and there's a bijection from $A$ to $B$, then if one of the sets is countable so is the other.
(b) A set $A$ is countable iff[14] there is an injective function $f : A \to \mathbb{P}$.

**proof (a)** We are supposing that there is a bijection from $A$ to $B$; give it a name; call it $g : A \to B$. The point about a bijection is that it matches the points of $A$ up with the points of $B$ with no doubling up and nothing missed out on either side. So if one of them is finite so is the other, with the same number of members. On the other hand, if $A$ is denumerable, there is a bijection $f : \mathbb{P} \to A$ (that's what 'denumerable' means) and $g \circ f : \mathbb{P} \to B$ is now a bijection (Corollary 9.4)[15], so that $B$ is also denumerable. On the other hand, if $B$ is denumerable, there is a bijection $h : \mathbb{P} \to B$, so that $h \circ g^{-1} : \mathbb{P} \to A$ is a bijection (because $g^{-1} : B \to A$ is a bijection, see Theorem 9.5) and $A$ is denumerable.

**(b)(i)** Suppose that $A$ is countable. Then it's either finite or denumerable. If it's finite, we can list it as $a_1, a_2, \dots, a_n$; now we can define $f : A \to \mathbb{P}$ by setting $f(a_1) = 1$, $f(a_2) = 2, \dots, f(a_n) = n$, and $f : A \to \mathbb{P}$ is injective. If $A$ is denumerable, there's a bijection $g : \mathbb{P} \to A$, and $g^{-1} : A \to \mathbb{P}$ is a bijection, therefore an injection.

**(ii)** Now suppose that there's an injective function $f : A \to \mathbb{P}$. In this case $\operatorname{ran} f$ is a subset of $\mathbb{P}$, and $f$ is a bijection from $A$ to $\operatorname{ran} f$. But $\mathbb{P}$ is denumerable, so $\operatorname{ran} f$ is countable (by Proposition 12.3) and $A$ is countable (by part (a) of this lemma).

The next fact is so fundamental that I'll call it a theorem.

**Theorem 12.5** (a) $\mathbb{P} \times \mathbb{P}$ is countable.
(b) If $A$ and $B$ are countable sets, so is $A \times B$.

**proof (a)** Remember that $\mathbb{P} \times \mathbb{P}$ is the set of all pairs $(m,n)$ where $m$, $n$ both belong to $\mathbb{P}$. Now we can list these by essentially the same method I used when listing the rational numbers, and in fact it's rather simpler. If we classify the pairs by the sum $m + n$, then there's only one pair with sum 2

(1,1);

there are two pairs with sum 3

(1,2), (2,1);

there are three pairs with sum 4

(1,3), (2,2), (3,1);

and so on, so if we use these as successive stages we get a list

(1,1), (1,2), (2,1), (1,3), (2,2), (3,1), (1,4), (2,3), ..., (4,1), (1,5), ...

which sooner or later will capture every pair $(m,n)$. So we have a full listing of $\mathbb{P} \times \mathbb{P}$, and $\mathbb{P} \times \mathbb{P}$ is denumerable.

[12]this is a synonym for 'obviously', see the last footnote.
[13]a Greek word, which in modern mathematics means 'something it's useful to know, but not specially interesting in itself'.
[14]'iff' is not a misprint. It's an abbreviation for 'if and only if'. It means that the sentence is telling you twice as much as you expected, and will take twice as long to prove.
[15]always check references. You'd be surprised how often they're wrong.

**(b)** If $A$ and $B$ are countable sets, there are injections $f_1 : A \to \mathbb{P}$ and $f_2 : B \to \mathbb{P}$ (Lemma 12.4(b)). Now look at the function $f : A \times B \to \mathbb{P} \times \mathbb{P}$ defined by saying that $f(a, b) = (f_1(a), f_2(b))$. This is also an injection, because if $f(a, b) = f(a', b')$ then $(f_1(a), f_2(b)) = (f_1(a'), f_2(b'))$, that is, $f_1(a) = f_1(a')$ and $f_2(b) = f_2(b')$; but $f_1$ and $f_2$ are injective, so $a = a'$ and $b = b'$, that is, $(a, b) = (a', b')$.

Now we have just seen that $\mathbb{P} \times \mathbb{P}$ is countable, so there is an injection $g : \mathbb{P} \times \mathbb{P} \to \mathbb{P}$. In this case, $g \circ f : A \times B \to \mathbb{P}$ is an injection (Theorem 9.3), so $A \times B$ is countable, by Lemma 12.4(b) in the other direction.

Once we have the result for two sets, it is an easy enough matter to prove that the direct product $A_1 \times A_2 \times \cdots \times A_n$ of finitely many countable sets is again countable. A formal proof follows quickly by an argument by induction on $n$, a topic which we will learn about in forthcoming lectures. I should mention though that it is *not* true that if we take an infinite list of countable sets $A_1, A_2, \cdots, A_n, \cdots$ and form the direct product of them all we obtain a countable set: in general we do not. Indeed, as long as an infinite number of the sets $A_i$ have at least 2 members, the infinite direct product turns out to be uncountable, though we will not prove this here.

The same kind of method gives us another of the fundamental theorems about countable sets.

**Theorem 12.6** If $A_1$, $A_2$, $A_3$, $\ldots$ are countable sets, then $A = A_1 \cup A_2 \cup A_3 \cup \ldots$ is still countable.

**proof** For each $n$, we have an injection $f_n : A_n \to \mathbb{P}$. I want to piece these together to give an injection from $A$ to $\mathbb{P} \times \mathbb{P}$, which ought to be trivial, but I think we have to watch it. The point is that the sets $A_n$ can easily overlap. So I think we need a rule like this:

if $x \in A$, let $n$ be the *first* number such that $x \in A_n$

(there has to be one, because that's what we mean by $A = A_1 \cup A_2 \cup \ldots$), and now

write $g(x) = (n, f_n(x))$.

It is supposed to be easy to see that $g$ is an injection from $A$ to $\mathbb{P} \times \mathbb{P}$; since there is an injection $h : \mathbb{P} \times \mathbb{P} \to \mathbb{P}$, there's an injection $h \circ g : A \to \mathbb{P}$, and $A$ is countable.

**Corollary 12.7** The union of two countable sets is countable.
(For we call our two sets $A_1$ and $A_2$, and then take the empty set for all the other $A_n$.)

We now have the machinery to decide for a good proportion of the sets arising in ordinary mathematics whether they're countable or not.

**Example 12.8** $= \{x \in \mathbb{R} : 0 < x < 1\} = ]0, 1[$ is uncountable[16].
**Reasoning:** $[0, 1] = ]0, 1[ \cup \{0, 1\}$. If $]0, 1[$ were countable, then $[0, 1]$, being the union of two countable sets would also be countable, but in 12.1-12.2 we proved by Cantor's Diagonal Argument that $[0, 1]$ is uncountable.

**Example 12.9** The set $\left]0, \frac{1}{2}\right[ = \{x \in \mathbb{R} : 0 < x < \frac{1}{2}\}$ is uncountable.
**Reasoning:** The set $]0, 1[$ of Example 12.4 is uncountable and the function $f : ]0, 1[ \to \left]0, \frac{1}{2}\right[$ defined by $f(x) = x/2$ is a bijection (check!). Hence by Lemma 12.4(a) $\left]0, \frac{1}{2}\right[$ is uncountable also.

**Example 12.10** The set $L$ of all linear equations of the form $ax + b = c$, where $a, b, c \in \mathbb{Q}$, is countable.
**Reasoning:** We can define a bijection $f : L \to \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$ by $(ax + b = c) \mapsto (a, b, c)$. Since $\mathbb{Q}$ is countable, so is $\mathbb{Q} \times \mathbb{Q}$ (by Theorem 12.5(b)) so $\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$ also is (by Theorem 12.5(b) again) and $L$ must be the same.

**Example 12.11** The set of all partial orders on the power set of the set of all relations on a finite set $A$.
**Reasoning:** This set is countable as it is finite! It certainly may be a monster but the set of all relations on $A$ is just $\mathcal{P}(A \times A)$; we take the power set of this giving $\mathcal{P}(\mathcal{P}(A \times A))$ which is still some finite set $F$ say. Finally every partial order on $F$ is a relation on $F$ and so the set of all partial orders on $F$ is a subset of $\mathcal{P}(F \times F)$, which again is finite. In fact, if $A$ has $n$ members then $A \times A$ has $n^2$ members; $\mathcal{P}(A \times A)$ has $2^{n^2}$ members; $F$ has $2^{2^{n^2}}$ members; $F \times F$ has $2^{2^{n^2+1}}$ members; and $\mathcal{P}(F \times F)$ has $2^{2^{2^{n^2+1}}}$ members, so the answer is less than that.

**Example 12.12** The range $\operatorname{ran} f$ of a function $f : A \to B$ where $A$ is countable.

[16] don't let these peculiar brackets ], [ worry you. In this course I'll explain them every time I use them.

**Reasoning:** This set $\operatorname{ran} f$ is countable (even though the codomain $B$ may be uncountable). For each $y \in \operatorname{ran} f$ choose just one member $x \in A$ such that $f(x) = y$, and call it $g(y)$. The mapping $g : \operatorname{ran} f \to A$ is a bijection from $\operatorname{ran} f$ onto some subset $S$ of $A$. Since $A$ is countable so is its subset $S$ by Proposition 12.3, and therefore $\operatorname{ran} A$ also is, by Lemma 12.4(a).

**Example 12.13** $C = (A \cup B) \cap (A \times A)$, where $A$ is denumerable.
**Reasoning:** $C$ is a countable set. Since $A$ is countable so is $A \times A$ by Theorem 12.5(b). Although we are told nothing about the set $B$, $C \subset A \times A$ and so is countable by Proposition 12.3. We cannot tell however whether $C$ is finite or denumerable.

**Example 12.14** The set $S$ of all points in the $xy$-plane.
**Reasoning:** We know that the interval $[0, 1]$ is uncountable. Now we have an injection $f : [0, 1] \to S$ defined by saying that $f(x)$ is to be the point with coordinates $(x, 0)$ in the plane. This function is a bijection between $[0, 1]$ and $\operatorname{ran} f$, so $\operatorname{ran} f$ is uncountable; but $\operatorname{ran} f$ is a subset of $S$, so $S$ must also be uncountable, by Proposition 12.3.

**Another uncountable set** The set $\mathcal{P}\mathbb{N}$ of all subsets of $\mathbb{N}$ is not countable.

**proof** I use the same strategy as in 12.1 above. Suppose that $f : \mathbb{P} \to \mathcal{P}\mathbb{N}$ is any function. Consider the set

$$A = \{n : n \in \mathbb{P},\, n \notin f(n)\}.$$

This is certainly a subset of $\mathbb{P}$ and therefore of $\mathbb{N}$, so $A \in \mathcal{P}(\mathbb{N})$. But if we look at any $n \in P$, then

either $n \in f(n)$, in which case $n \notin A$, so $f(n) \neq A$,

or $n \notin f(n)$, in which case $n \in A$, so again $f(n) \neq A$.

In fact we always have $n \in A \triangle f(n)$, so $f(n)$ is never equal to $A$, and we have a member of $\mathcal{P}\mathbb{N}$ which is not a value of $f$. Thus there is no surjection from $\mathbb{P}$ to $\mathcal{P}\mathbb{N}$ and $\mathcal{P}\mathbb{N}$ is not countable.

**Remark** A useful way of thinking about the difference between 'countable' and 'uncountable' sets is by the way in which their members can be handled by computers. A computer aims to store integers exactly. Of course it can't handle big ones, but that's only a matter of storage allocation; when you get an 'integer overflow' message, it's a call to re-write your program, not a reason to give up. Ordinary computers have instructions on handling integers, positive and negative, with exact arithmetic; and this is possible because $\mathbb{Z}$ is countable. For real numbers, however, you have to use floating-point arithmetic, and while you can always call for double or even quadruple precision the answers are necessarily unreliable in the last couple of digits. There is absolutely no way round this problem, because the set $\mathbb{R}$ is uncountable. You can't describe even a *single* real number in finitely many symbols, unless it happens to be a particularly easy one like 0 or $\frac{2}{3}$ or $-1.234$. On the other hand, so long as you are working with rational numbers only, you can ask for exact calculation (the MAPLE program will do this for you, for instance), because $\mathbb{Q}$ is countable.

The next thing to note is that $A \times A$ is countable whenever $A$ is, but that $\mathcal{P}\mathbb{N}$ (for instance) is not. This corresponds to the fact that (for large numbers $n$) $n^2$ is very much smaller than $2^n$. You can, I suppose, imagine counting a pack of playing cards to find out if it's complete; 52 is the sort of number you can deal with bare-handed, so to speak. If you want to deal with $52^2 = 2704$ objects, you would probably want machine assistance; but any computer can handle a list of 2704 things without blinking, and even $2704^2 \doteq 7$ million is not an impossible problem nowadays. But if you want to look at all *subsets* of a pack of playing cards, you have to consider $2^{52}$ possibilities, which is out of reach. There is an important topic ('complexity') in theoretical computing which studies just which problems are likely to be accessible to brute-force methods, and this is dominated by calculations of this kind. In particular, if your sets are generated by taking products of smaller sets, you're in with a chance; but if they're got by taking power sets, you're not.

Version of 15.10.99

**Some Algebra**

A lot of tricky algebraic manipulations that people feel unsure about involve factorisation and their justification centres on the Distributive Law. This is the one that I shall focus on in this lecture. The Distributive Law is the most peculiar and least obvious of all the Laws of Algebra. Its peculiarity lies in the fact that it is the only one that links the two main operations of arithmetic, addition and multiplication: it is the law which tells you how to multiply out brackets.

$$a(b+c) = ab + ac$$

For example $4(2+3) = 4 \times 2 + 4 \times 3$, which is certainly true as $4(2+3) = 4 \times 5 = 20 = 8 + 12$. It's worth thinking about this rule a little. On one side of this sum we have:

$$4(2+3) = (2+3) + (2+3) + (2+3) + (2+3)$$

while the other is

$$(2+2+2+2) + (3+3+3+3)$$

Both sums involve the same numbers but merely added in a different order which of course makes no difference (that is a law too: the Commutative Law of Addition: $a + b = b + a$. As long as we are dealing with positive numbers, the general case holds for the same reason: it says just that

$$\underbrace{(b+c) + (b+c) + \cdots + (b+c)}_{a\ times} = \underbrace{(b+b+\cdots+b)}_{a\ times} + \underbrace{(c+c+\cdots+c)}_{a\ times}$$

The subtlety in the Distributive Law comes from using it in the reverse direction to express a sum as a product by 'taking out' a common factor. Unlike expansion of brackets, an entirely mechanical process, factorisation involves considering an expression and spotting a common factor.

We can now expand an expression such as $(x+y)^2$. For the moment, let $a$ stand for the number $x + y$. Then

$$(x+y)^2 = (x+y)(x+y) = a(x+y) = ax + ay$$

Now $ax = xa = x(x+y) = x^2 + xy$, similarly $ay = ya = y(x+y) = yx + y^2$. Combining all this yields:

$$(x+y)^2 = ax + ay = x^2 + xy + yx + y^2 = x^2 + xy + xy + y^2 = x^2 + 2xy + y^2$$

The Distributive Law also lies at the bottom of the process of placing a fraction over a common denominator. The expressions may be complicated but numerators and denominators still stand for (unspecified) numbers and so are subject to the same Laws of Algebra. Consider the addition of two fractions:

$$\frac{a}{b} + \frac{c}{d}$$

The number $bd$ is a multiple of both $b$ and $d$ (perhaps not the least multiple) so $bd$ can act as a common denominator (perhaps not the lowest). We multiply the denominator $b$ by $d$ and so we multiply the numerator by $d$ as well. The overall effect is to multiply the first fraction by $\frac{d}{d} = 1$ which does not change its value. Similarly we multiply $\frac{c}{d}$ by $\frac{b}{b}$ to give:

$$\frac{ad}{bd} + \frac{cb}{db}$$

Now that our fractions have the same denominator we may add the numerators to get

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

This last stage is itself a statement of the Distributive Law. To see it this way ask yourself what is being said when we write something like:

$$\frac{a+b}{c} = \frac{a}{c} + \frac{b}{c}?$$

Division by $c$ means multiplication by the reciprocal $d = \frac{1}{c}$. Hence this last statement becomes:

$$d(a+b) = da + db$$

which is the Distributive Law.

The system of positive counting numbers is inadequate for algebra because two natural operations, subtraction and division, take you out of the system. Division leads to fractions and learning the arithmetic of fractions is quite difficult but is more readily accepted because it can be demonstrated explicitly using physical objects such as slices of pie. Negative numbers took much longer to gain acceptance. Even during the Renaissance the validity of their use was questioned because they seemed to lack physical interpretation. Negative numbers are accepted as more meaningful in the modern world, perhaps because we are so familiar with the notion of debt, which is the interpretation of negative money. It is certainly true that people feel debt to be real so the arithmetic of debt, which must at least allow for the addition of negative sums, is accepted. Debts grow larger when subject to interest. This involves multiplication of these negative values by positive multipliers to yield larger debt: if you have a \$100 overdraft at 30% penalty interest you will have an account worth $\$(-100 \times 1.3) = -\$130$ one year later.

A psychological sticking point however seems to be admitting that the product of two negative numbers is positive. This is exactly what you need to do in order that your algebra be consistent. For example $(2-1)(2-1) = 1 \times 1 = 1$. Treating subtraction as adding the opposite we also have:

$$1 = (2-1)(2-1) = (2+-1)(2+-1)$$

Using the Distributive Law we expand the brackets by multiplying each term in the first bracket by each in the second and sum them all, giving 4 terms in all. The calculation continues:

$$\begin{aligned} &= (2 \times 2) + (2 \times -1) + (-1 \times 2) + (-1 \times -1) \\ &= 4 + -2 + -2 + (-1 \times -1) = 0 + (-1 \times -1) = -1 \times -1. \end{aligned}$$

Thus we are led to $1 = -1 \times -1$; anything else will yield the wrong answer.

The rules therefore need to be that the product of two numbers of the same sign is positive, while the product of numbers with opposite signs is negative. We can now expand any product of brackets using the Distributive Law and these rules. To expand a bracket involving a subtraction we treat the minus as meaning addition of the opposite: we just need to realise that $(-a)b = a(-b) = -(ab)$ as each is the opposite of the product $ab$:

$$a(b-c) = a(b+(-c)) = ab + a(-c) = ab - ac$$

For example:

$$(x-y)^2 = (x-y)(x-y) = x(x-y) - y(x-y) = x^2 - xy - yx - y(-y)$$

Now subtracting $y(-y)$ means adding $(-y) \times (-y) = y^2$, and so we obtain:

$$(x-y)^2 = x^2 - 2xy + y^2.$$

In a similar way we derive the expression for the Difference of Two Squares:

$$(x+y)(x-y) = x(x-y) + y(x-y) = x^2 - xy + yx - y^2 = x^2 - y^2$$

Again, it is the use of this in the reverse direction which often needs to be appreciated. The difference of two squares can be written as a product. For example:

$$n^2 - 1 = n^2 - 1^2 = (n+1)(n-1).$$

Version of 5.10.00

**Introduction to Induction**

For the next couple of lectures I shall be talking about *proofs by induction*, and I think it might help if I try to address some obvious questions straight away, because this is going to be hard work, and if you don't know why I'm asking you to do it it will be hard for you to do your best.

Question 1. What is a *proof*?

Question 2. What is a proof by *induction*?

Question 3. Why does anybody bother with proofs?

Question 4. Why do we have to bother with proofs?

The first three are the easy ones. (1) A proof is a logical argument which assures us that what we are saying is true. (3) Pure mathematicians, at least, like to know that what they are saying is true. (2) See below.

The hard question is (4). If you are happy to believe everything your teachers tell you, you hardly need to be able to prove any of it yourselves. After all, for quite a lot of what we are trying to teach you, the proofs are really very difficult, and we are going to ask you to take it on trust anyway. But if you are ever going to try to do anything new by yourself, then it would be a good thing if you had at least some notion of how to check that you're getting it right. And the particular kind of new thing that many of you will want to be able to do, is to write computer programs which actually work. You will know already that as soon as you have written more than two lines of code, there is a serious danger that you've made a mistake. You will have heard of the expensive blunders which have been attributed to software errors. The Holy Grail of theoretical computing is an effective technique for deciding, before live testing, whether a particular program will deliver the goods as advertised. The general problem is undoubtedly so difficult that none of us can really expect to solve it. But there are plenty of little questions which *can* be solved, and the centre of many solutions is a proof by induction, which is where we came in.

Now for Question 2: What is a proof by induction? Let's begin with an example. This may sound like a bad idea as how can we work an example before we are introduced to the technique? What we shall do is to tackle a simple example and with luck you will see how the general approach emerges from what you might naturally do when grappling with a problem like this.

The problem is to verify the following formula for summing positive integers.

$$1 + 2 + 3 + \ldots + n = \tfrac{1}{2}n(n+1) \tag{1}$$

The natural thing for a good sceptical student to do is to test (1) for a few values of $n$. If we put $n = 1$ we get the formula

$$1 = \frac{1}{2} \times 1 \times (1+1)$$

and if we put $n = 2$ we get the formula

$$1 + 2 = 3 = \tfrac{1}{2} \times 2 \times (2+1)$$

which are both true. It is very easy to test several more values of $n$ and most people would conclude that the general formula is pretty safe. But look: suppose you were writing a program for a supermarket. You have carefully checked your formula for every number $n$ from 1 to 100. But sooner or later the program you have written is going to be applied to a number you've never heard of. How can you be absolutely sure that the formula will still work?

It quite often happens that if you check some more small values of $n$, and look carefully at what you are doing, you can get a clue to why it might go on working for ever. Let's look at the cases $n = 3$, 4, 5:

$$1 + 2 + 3 = 6 = \tfrac{1}{2} \times 3 \times (3+1),$$

$$1 + 2 + 3 + 4 = 10 = \tfrac{1}{2} \times 4 \times (4+1),$$

$$1 + 2 + 3 + 4 + 5 = 15 = \tfrac{1}{2} \times 5 \times (5+1).$$

Now the clue, which turns out to be the essential idea, is that when working out $1+2+3+4+5$ you don't (I hope) start again at the beginning. What you do is to say that you already know what $1+2+3+4$ is, that's 10, so all you have to do is to add another 5 and that makes 15. Well now: what happens if you notice not only that $1+2+3+4=10$ but that $10=\frac{1}{2}\times 4\times(4+1)$? Then you will get

$$1+2+3+4+5=10+5=(\frac{1}{2}\times 4\times 5)+5. \tag{2}$$

Well, there are two 5's in the right-hand formula, so we can collect them together:

$$1+2+3+4+5=((\frac{1}{2}\times 4)+1)\times 5$$

(this is the Distributive Law again)

$$=\frac{1}{2}\times(4+2)\times 5 \tag{3}$$

(and again!)

$$=\frac{1}{2}\times 6\times 5=\frac{1}{2}\times 5\times 6$$

which is what we expected it to be. Now if you look at this, it seems to depend on a couple of accidents. First, we had 5 turning up twice in equation (2), and then in equation (3) we had a $4+2$ in just the right place to be turned into a 6. So we had better try it again:

$$\begin{aligned}1+2+3+4+5+6&=(1+2+3+4+5)+6\\&=(\frac{1}{2}\times 5\times 6)+6 &(2')\\&=((\frac{1}{2}\times 5)+1)\times 6\\&=\frac{1}{2}\times(5+2)\times 6 &(3')\\&=\frac{1}{2}\times 7\times 6=\frac{1}{2}\times 6\times 7\end{aligned}$$

Once again, the 6 appeared twice in equation $2'$, and $5+2$ appeared where we needed a 7.

Can we think of some good reason why this should *always* work?

What is happening here is that we've found some number $k$ say such that

$$1+2+\ldots+k=\frac{1}{2}\times k\times(k+1).$$

When we go one step farther, we are looking at

$$\begin{aligned}1+2+\ldots+(k+1)&=(1+2+\ldots+k)+(k+1)\\&=(\frac{1}{2}\times k\times(k+1))+(k+1) &(2^*)\\&=((\frac{1}{2}\times k)+1)\times(k+1)\\&=\frac{1}{2}\times(k+2)\times(k+1) &(3^*)\\&=\frac{1}{2}\times((k+1)+1)\times(k+1)=\frac{1}{2}\times(k+1)\times((k+1)+1),\end{aligned}$$

which is the shape that our general formula takes when we write $k+1$ for $n$.

At this point we do have, in a rather disorganised way, a proof by induction. We *checked* at least one case at the bottom. (Actually we checked several, no harm in that, and in fact a useful precaution, because trying to prove something by induction when it isn't true will get you *no* marks.) Then, after a bit of experiment, we found a *general method* to show that

*if* $1+\ldots+k=\frac{1}{2}\times k\times(k+1)$

*then* $1+\ldots+(k+1)=\frac{1}{2}\times(k+1)\times((k+1)+1)$.

(That's what the last solid block of algebra is doing.) Now we can argue as follows.

The formula (1) is true when $n=1$.
If the formula (1) is true when $n=k$, it is true when $n=k+1$.
So it is true when $n=1+1=2$.
So it is true when $n=2+1=3$.
So it is true when $n=3+1=4$.
So it is true when $n=5$.
So it is true when $n=6$.
So it is true when $n=7$.
So ...

This process really will go on as long as we want it to, because the formulae in ($2^*$)-($3^*$) work for all numbers $k$; not just the ones we've looked at, not just the ones someone sometime has looked at, not just the ones someone sometime will look at, but *all*. So it won't matter if one day the supermarket manages to get $1+2+3+\ldots+7136$ ball-bearings into the biggest display on earth. There will still be $\frac{1}{2}\times 7136\times 7137$ ball-bearings in the pile.

Now let me try to explain the general approach of which this is an example.

**First Principle of Mathematical Induction** Let $\mathrm{P}(1), \mathrm{P}(2), \ldots, \mathrm{P}(n), \ldots$ be a sequence of propositions, one for each positive integer $n$. Suppose that:

(i) $\mathrm{P}(1)$ is true;

**(base step)**

(ii) $\mathrm{P}(k+1)$ is true whenever $\mathrm{P}(k)$ is true.

**(inductive step)**

Then $\mathrm{P}(n)$ is true for all $n=1,2,3,\ldots$.

We close this lecture with a second similar application.

**Example 14.1** Suppose that $\mathrm{P}(n)$ is the statement

$$\frac{1}{1\times 2}+\frac{1}{2\times 3}+\ldots+\frac{1}{n(n+1)}=\frac{n}{n+1}\ \forall\, n=1,2,\ldots.$$

**Base Step:** First verify the first statement in the sequence. $\mathrm{P}(1)$ says that

$$\frac{1}{1\times 2}=\frac{1}{1+1}. \qquad \mathrm{P}(1)$$

This is true as both sides simplify to $\frac{1}{2}$.

**Inductive Step:** Assume that for some value $k$ of $n$, $k\geq 1$, $\mathrm{P}(k)$ is true; that is we assume that

$$\frac{1}{1\times 2}+\frac{1}{2\times 3}+\ldots+\frac{1}{k(k+1)}=\frac{k}{k+1}. \qquad \mathrm{P}(k)$$

Now look at what $\mathrm{P}(k+1)$ says:

$$\frac{1}{1\times 2}+\frac{1}{2\times 3}+\ldots+\frac{1}{k(k+1)}+\frac{1}{(k+1)(k+2)}=\frac{k+1}{k+2} \qquad \mathrm{P}(k+1)$$

Take the left-hand formula, and try to simplify it:

$$\frac{1}{1\times 2}+\frac{1}{2\times 3}+\ldots+\frac{1}{k(k+1)}+\frac{1}{(k+1)(k+2)}$$
$$=(\frac{1}{1\times 2}+\frac{1}{2\times 3}+\ldots+\frac{1}{k(k+1)})+\frac{1}{(k+1)(k+2)}$$

(collecting the first $k$ terms together)

$$=\frac{k}{k+1}+\frac{1}{(k+1)(k+2)}$$

(using the **inductive hypothesis** $\mathrm{P}(k)$ to simplify the formula)

$$=\frac{k(k+2)+1}{(k+1)(k+2)}$$

(using the Distributive Law once more)

$$=\frac{k^2+2k+1}{(k+1)(k+2)}$$
$$=\frac{(k+1)^2}{(k+1)(k+2)}=\frac{k+1}{k+2}=\frac{k+1}{((k+1)+1)},$$

which is what $\mathrm{P}(k+1)$ said.

So we see that

(i) $\mathrm{P}(1)$ is true,

(ii) whenever $\mathrm{P}(k)$ is true, so is $\mathrm{P}(k+1)$,

and we can conclude that

$\mathrm{P}(n)$ is true for every integer $n \geq 1$,

that is, that

$$\tfrac{1}{1\times 2}+\tfrac{1}{2\times 3}+\tfrac{1}{3\times 4}+\ldots+\tfrac{1}{n(n+1)}=\tfrac{n}{n+1}$$

for every integer $n \geq 1$.

Version of 5.10.00

**Induction Examples**

The Principle of Induction is often likened to the toppling of a row of dominoes. They all fall down because the first one is pushed, knocking over the second, which falls into the third, which in turn knocks over the fourth and so on. Toppling the first domino corresponds to proving the Base Step. To be sure that all will fall over we next perform the inductive step: this would involve checking that the separation of an arbitrary pair of successive dominoes was less than the length of each domino (a necessary step, for if it should not be so at any stage then the inductive argument, and with it the toppling of all the dominoes, would fail).

It quite often happens that we have a sequence of propositions $\mathrm{P}(0)$, $\mathrm{P}(1)$, $\mathrm{P}(2)$, $\ldots$ starting with $\mathrm{P}(0)$ rather than $\mathrm{P}(1)$. In this case the 'base step' has to be the case $n = 0$, and the 'inductive step' from $k$ to $k + 1$ has to be done for every integer $k \geq 0$ rather than for every $k \geq 1$. On other occasions, the propositions we're interested in may start with $\mathrm{P}(2)$, or even later; but the method doesn't change; we just pick the appropriate level for our base step, and watch the inductive step to make sure that it works when it's needed.

**Example 15.1** Prove that $2^n > n^2\ \forall\ n \geq 5$.

Before we start, it is perhaps worth noting that $2^n > n^2$ is false for $n = 1, 2, 3, 4$, so that $n = 5$ is indeed the natural starting point. The base to anchor our induction is then:

**Base Step**

$$2^5 > 5^2 \qquad \text{P}(5)$$

which is certainly true, since $2^5 = 32 > 25 = 5^2$.

**Inductive Step** Suppose that $2^k > k^2$ for some $k \geq 5$. Our task is to verify that this implies that $2^{k+1} > (k+1)^2$. In this case it is not so easy to relate the LHS of $\text{P}(k)$ to that of $\text{P}(k+1)$. We do the obvious thing nevertheless, multiply both sides of $\text{P}(k)$ by 2 to obtain:

$$2^{k+1} > 2k^2.$$

This statement is a valid deduction from $\text{P}(k)$ and does at least say something about the LHS of $\text{P}(k+1)$. Now we have the wrong RHS, but perhaps we can find some way of comparing $2k^2$ with $(k+1)^2$. (Remember that *building* a mathematical proof always involves a lot of blundering in the dark. You mustn't expect always to see your way through without trying several blind alleys.) One way of doing this is to look at $2k^2 - (k+1)^2$:

$$\begin{aligned} 2k^2 - (k+1)^2 &= 2k^2 - (k^2 + 2k + 1) \\ &= 2k^2 - k^2 - 2k - 1 \\ &= k^2 - 2k - 1 \\ &= k(k-2) - 1. \end{aligned}$$

(Here the first three steps are just following our noses. Whenever you see $(k+1)^2$ in a formula, you can try changing it into $k^2 + 2k + 1$ and seeing what happens. The last step isn't so obvious, and in fact there are plenty of other things which work; but one way of looking at the whole string is to say that we're looking for the formula *with fewest multiplications in it.* The point about the last line is that there's only one multiplication, and that's what makes it manageable.) Now remember that we're only interested in $k \geq 5$. And if $k \geq 5$ then $k - 2 \geq 3$ so $k(k-2) \geq 15$ and $k(k-2) - 1 \geq 14$.

Actually this is more than we really need to know. All that matters is that, if $k \geq 5$, then

$$2k^2 - (k+1)^2 \geq 0,$$

so that

$$2k^2 \geq (k+1)^2.$$

We now have the component parts of our proof; let's put them together neatly:

Assume that $k \geq 5$, and that $\text{P}(k)$ is true, that is, that $2^k > k^2$. Then, because

$$2k^2 - (k+1)^2 = k(k-2) - 1 \geq 14,$$

$2^{k+1} > 2k^2$ and $2k^2 \geq (k+1)^2$, so $2^{k+1} > (k+1)^2$, that is, $\text{P}(k+1)$ is true.

**Example 15.2** Show that $n(n^2 + 5)$ is divisible by 6 for all $n = 1, 2, \cdots$.

**Base Step**

$$6 | (1 \times (1^2 + 5)) \qquad \text{P}(1)$$

is true, because $1 \times (1^2 + 5) = 6$ is a multiple of 6 (it's $6 \times 1$).

**Inductive step**

Assuming $\text{P}(k)$, that is, that $6 | k(k^2 + 5)$, we want to prove that $6 | (k+1)((k+1)^2 + 5)$.

It's a bit like last time; we are assuming something about the formula $k(k^2 + 5)$ and we want to prove something about the similar formula $(k+1)((k+1)^2 + 5)$. Now it helps to have a mental picture of what we're looking for. The multiples of 6 are

$$\ldots, -12, -6, 0, 6, 12, 18, 24, \ldots.$$

(For this problem, of course, we're not interested in the negative ones, because we know that $n(n^2+5)$ will be positive for any positive $n$.) But the point is that if you add or subtract two multiples of 6 you get another one. So once again the thing to do is to look at the *difference* $(k+1)((k+1)^2+5) - k(k^2+5)$. If this is divisible by 6, we'll be home. Now we have a bit of algebra to do, but the only real problem is not making a silly mistake:

$$\begin{aligned}
(k+1)((k+1)^2+5) - k(k^2+5) &= (k+1)(k^2+2k+1+5) - (k^3+5k) \\
&= (k+1)(k^2+2k+6) - (k^3+5k) \\
&= k(k^2+2k+6) + (k^2+2k+6) - (k^3+5k) \\
&= k^3+2k^2+6k+k^2+2k+6-k^3-5k \\
&= 3k^2+3k+6 \\
&= 3k(k+1)+6.
\end{aligned}$$

This doesn't look quite good enough. The 6 on the end is OK, but it looks as if what we have is a multiple of 3, not a multiple of 6. But wait! when you take $k(k+1)$, one of the factors has to be an even number. We don't know which, because we don't know what $k$ is (this has got to work for *every* $k \geq 1$, with no gaps), but either $k$ is even, and we're home, or $k$ is odd, and $k+1$ is even. So $k(k+1)$ is always even, and $3k(k+1)$ is always a multiple of 6, and $3k(k+1)+6$ is always a multiple of 6.

So this is going to work. Once again, write it out prettily:

Assume that $k \geq 1$, and that $\mathrm{P}(k)$ is true, that is, that $k(k^2+5)$ is divisible by 6. Then, because $k(k+1)$ is even,

$$\begin{aligned}
(k+1)((k+1)^2+5) &= k^3+3k^2+8k+6 \\
&= k(k^2+5)+3k(k+1)+6
\end{aligned}$$

is a sum of three multiples of 6, so is itself a multiple of 6, and $\mathrm{P}(k+1)$ is true.

**Example 15.4** Generalized Distributive Law for Sets: for any set $A$ and any $n$ sets $B_1, B_2, \cdots, B_n$, where $n \geq 1$,

$$A \cap (B_1 \cup B_2 \cup \cdots \cup B_n) = (A \cap B_1) \cup (A \cap B_2) \cup \cdots \cup (A \cap B_n).$$

**Proof Base step**

$$A \cap B_1 = A \cap B_1 \qquad \mathrm{P}(1)$$

is true.

**Inductive step** Assuming $\mathrm{P}(k)$, that is, that

$$A \cap (B_1 \cup B_2 \cup \cdots \cup B_k) = (A \cap B_1) \cup (A \cap B_2) \cup \cdots \cup (A \cap B_k),$$

we have to prove $\mathrm{P}(k+1)$, that is, that

$$A \cap (B_1 \cup B_2 \cup \cdots \cup B_{k+1}) = (A \cap B_1) \cup (A \cap B_2) \cup \cdots \cup (A \cap B_{k+1}).$$

Actually this is very like the argument for $1+2+\ldots+n$ last lecture. The point is that in the RHS

$$(A \cap B_1) \cup (A \cap B_2) \cup \cdots \cup (A \cap B_{k+1})$$

of $\mathrm{P}(k+1)$, what we've got is the RHS of $\mathrm{P}(k)$ with one term added. So let's use it:

$$\begin{aligned}
&(A \cap B_1) \cup \ldots \cup (A \cap B_{k+1}) \\
&\qquad = ((A \cap B_1) \cup \ldots \cup (A \cap B_k)) \cup (A \cap B_{k+1}) \\
&\qquad = (A \cap (B_1 \cup \ldots \cup B_k)) \cup (A \cap B_{k+1})
\end{aligned}$$

because $\mathrm{P}(k)$ is supposed to be true. But at this point we notice that we can apply the Distributive Law of Sets (§4b of the list at the beginning of the course) to see that

$$\begin{aligned}(A \cap B_1) \cup \ldots \cup (A \cap B_{k+1}) \\ &= (A \cap (B_1 \cup \ldots \cup B_k)) \cup (A \cap B_{k+1}) \\ &= A \cap ((B_1 \cup \ldots \cup B_k) \cup B_{k+1}) \\ &= A \cap (B_1 \cup \ldots \cup B_k \cup B_{k+1}),\end{aligned}$$

which is what we were trying to prove.

Version of 5.10.00

**Recursions and Fibonacci Numbers**

The French proverb, 'Step by step we can go a long way' is nowhere more true than in mathematics. In particular, a huge raft of constructions in computing are recursive - that is to say are built step-by-step and the check that the final object has all the specifications that we intend is normally a proof by induction. Recursive processes are tailor made for such proofs. Once again the examples here will mostly involve sequences of numbers but in practice the members of recursively defined sequences can consist of any mathematical or computational objects that you might meet. For that reason it is important to feel completely at home with recursive processes and the inductive arguments that accompany them.

**Example 16.1** $n$ lines are drawn on a sheet of paper so that every pair intersect but no three are concurrent (that is, no three meet in a common point). Write down an expression for $a_n$, the number of regions into which the sheet is divided by the $n$ lines, in terms of $a_{n-1}$ and thus find a formula for $a_n$ in terms of $n$ only.

It is simple to write down the first few values of $a_n$:

$$a_1 = 2, \quad a_2 = 4, \quad a_3 = 7, \ldots$$

Nevertheless the emerging pattern of the number of regions is not so clear. Let us examine what happens as we pass from the stage where there are $n-1$ lines to that where there are $n$ lines. The $n$th line splits $n$ regions: before, between and after the $n-1$ intersection points with the first $n-1$ lines, creating overall an increase in the number of regions of $n$. (Look carefully at the $n = 3$ case to convince yourself of this.) We therefore have the following *recursion*:

$$a_n = a_{n-1} + n \;\forall\; n = 2, 3, 4 \ldots, \quad a_1 = 2.$$

This recursion involves expressing $a_n$ in terms of the previous term. To be fully specified therefore we do need also to state the *initial value* of $a_1$. This is called specifying the *initial conditions* of the recursion; for some recursions, as we shall see, more than one initial value needs to be given for the recursive sequence to be fully specified.

Applying this recursion to $a_{n-1}$ allows us to write:

$$a_n = (a_{n-2} + (n-1)) + n$$

Applying the recursion again to $a_{n-2}$ and to the subsequent earlier values of $a_k$ that then arise gives:

$$\begin{aligned}a_n &= a_1 + 2 + 3 + 4 + \ldots + (n-1) + n \\ &= 2 + 2 + 3 + 4 + \ldots + (n-1) + n.\end{aligned}$$

Now, our first example of an inductive problem was the proof that $1 + 2 + 3 + \ldots + (n-1) + n = \frac{1}{2}n(n+1)$ and so we conclude that:

$$a_n = 1 + \frac{1}{2}n(n+1) = \frac{2 + n + n^2}{2}.$$

**Example 16.2** The Tower of Hanoi. This is a classical problem which begins with a board with 3 fixed pegs and $n$ circular rings. The rings are all of different diameters and are arranged in a tower initially sitting on Peg A say. Your task is to construct a similarly tapering pile on Peg C by transferring rings amongst the pegs subject to the following natural rules of movement:

1. Only one ring may be moved at a time;
2. No ring may be placed on top of a smaller ring.

Our task is to find the minimum number of moves $a_n$ required to play the Tower of Hanoi.

By playing the game with a few coins you will soon see that $a_1 = 1$, $a_2 = 3$ and $a_3 = 7$. This may also help you see the key to the recursion. In order to play the $n$-ring game, you have got to move the bottom ring. You can only do this if you have first shifted all the other rings to one of the other piles, and this will take at least $a_{n-1}$ moves. Then, after moving the bottom ring, taking 1 move, you'll have to shift the pile of rings back on top of it, which will take at least $a_{n-1}$ moves again. So at the very best you will need $2a_{n-1} + 1$ moves; that is, $a_n \geq 2a_{n-1} + 1$. Can we actually do it as slickly as that? Yes, provided we move the $n-1$ upper rings to peg $B$ (not $C$!), so that $C$ is now free to take the bottom ring, and then move the others from peg $B$ to peg $C$. So $a_n = 2a_{n-1} + 1$ exactly, while $a_1 = 1$.

Armed with our recursion, we can inspect the sequence of $a_n$'s for some more values in order to find a solution of the recurrence that we can then verify inductively.

$$a_1 = 1, \quad a_2 = 3, \quad a_3 = 7, \quad a_4 = 15, \quad a_5 = 31, \quad a_6 = 63, \quad a_7 = 127, \quad \ldots$$

See the pattern? It is:

$$a_n = 2^n - 1.$$

This certainly holds for the first few values of $n$ and using the recursion we can verify by induction that it always holds. The statement $\mathrm{P}(n)$ is '$a_n = 2^n - 1$'; the base step is to look at

$$a_1 = 2^1 - 1 \qquad \mathrm{P}(1)$$

which is true, because $a_1 = 1 = 2 - 1$; and the inductive step is

$$a_{k+1} = 2a_k + 1$$

(applying our recursion relation with $n = k + 1$)

$$= 2(2^k - 1) + 1$$

(by the inductive hypothesis $\mathrm{P}(k)$)

$$= 2^{k+1} - 2 + 1 = 2^{k+1} - 1,$$

so that $\mathrm{P}(k+1)$ is true.

(How long would it take you to finish the 20-peg game at 100 moves per day?)

Our third example of a recursion is Fibonacci's[17] Rabbit Problem (13th century). At the beginning of the first month we have one newborn pair of rabbits. Each pair will give birth to another pair at the end of their second month of life, and at the end of every month after that (Fibonacci's Rabbits are immortal). Investigate the value of $a_n$, the number of pairs at the beginning of month $n$.

This is an easy question to answer for the first few particular values of $n$. It is difficult to find a formula for $a_n$ in terms of $n$ itself. We can however find a *recursion* for $a_n$, a way of expressing $a_n$ in terms of earlier values of the sequence, which will be most useful and which does lead to a formula for the $a_n$, which turns out to be of a very surprising form.

At the beginning of month 1 there is 1 pair, and the same is true at the start of the second month as the pair has not yet reached maturity. Hence we have $a_1 = a_2 = 1$. However we see that $a_3 = 2$ as at the end of the second month a new pair is born. Similarly we see that $a_4 = 3$ (because the first pair of rabbits have produced two more offspring, but their babies haven't yet) while $a_5 = 5$ as at the end of the 4th month there are now 2 fertile pairs giving birth to 2 new pairs. The general picture is as follows. At the beginning

[17]Leonardo Pisano Fibonacci, 1170-1250; `http://www-history.mcs.st-and.ac.uk/history/Mathematicians/Fibonacci.html`

of the $n$th month the number of pairs will equal $a_{n-1}$, the number of pairs that we had at the beginning of the previous month, together with one new pair for each reproducing pair. The number of reproducing pairs equals the number of pairs which are at least 2 months old - this is equal to $a_{n-2}$, the number of pairs we had 2 months ago which are now all at least 2 months old. We therefore obtain a simple equation governing the number of pairs $a_n$:

$$a_n = a_{n-1} + a_{n-2},\ n = 3, 4, 5, \dots .$$

Note that this recursion makes sense only for $n \geq 3$ as the argument from which the recursion is derived assumes that there are 2 previous months with which to work. The recursion certainly allows us to calculate $a_n$ for small values of $n$ very easily. The first 16 Fibonacci numbers are:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, \dots$$

Actually it is a little easier to work with the Fibonacci Sequence by starting with $a_0 = 0$; this is still consistent with the above recursion which now first applies when $n = 2$: $a_2 = a_1 + a_0$ as $1 = 1 + 0$. We shall do this in future. Many properties of Fibonacci Numbers can be proved using the above recursion and induction. For example, the Fibonacci numbers certainly grow rapidly but we can prove the following bound to their growth.

**Example 16.3** Show that $a_n \leq 2^{n-1}\ \forall n \geq 0$.

The facet of this induction which is different from examples from the two previous lectures is that, because of the nature of the recursion, the inductive step will involve the assumption of the inductive hypothesis holding for not just the previous case but the two previous cases. This means that it will be necessary to check the first two cases directly in the base step and not just the first. Once we appreciate this however, there is no real difficulty in proceeding.

**Base Step** For $n = 0$ we have $a_0 = 0 \leq \frac{1}{2} = 2^{0-1}$; $a_1 = 1 = 2^0$, and so the statement '$a_n \leq 2^{n-1}$' holds for the cases $n = 0$ and $n = 1$.

**Inductive Step** Consider $\mathrm{P}(k) : a_k \leq 2^{k-1}$ for some $k \geq 2$ and assume that *both* $\mathrm{P}(k-1)$ and $\mathrm{P}(k-2)$ hold. Then by the recursion we certainly have:

$$\begin{aligned} a_k &= a_{k-1} + a_{k-2} \\ &\leq 2^{(k-1)-1} + 2^{(k-2)-1} \end{aligned}$$

(because both $\mathrm{P}(k-1)$ and $\mathrm{P}(k-2)$ are supposed to be true)

$$\begin{aligned} &= 2^{k-2} + 2^{k-3} \\ &\leq 2^{k-2} + 2^{k-2} \\ &= 2^{k-1}, \end{aligned}$$

so that $a_k \leq 2^{k-1}$, that is, $\mathrm{P}(k)$ is true.

How about a formula for the Fibonacci Numbers? We shall answer this intriguing question next time.

Version of 5.10.00

There is a standard theory that provides the solution of any so-called difference equation of the form:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2}.$$

The Fibonacci Recurrence is one of this type: put the constants $c_1$ and $c_2$ both equal to 1. We shall not however have time to develop this theory in this course. It in fact applies more generally to so-called linear recursions with constant coefficients involving perhaps more than 2 terms. Note that if a recursion involves say 3 previous terms then any inductive argument concerning it would require the direct checking of the first 3 terms in the Base Step.

We can nevertheless state and verify the rather preposterous formula for the $n$th Fibonacci number without explaining how it was ever found in the first place.

$$a_n = \frac{1}{\sqrt{5}}\Big((\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n\Big)$$

This is really a fright the first time you see it: after all, there is no obvious reason why the monster on the right should turn out to be an integer at all, never mind the $n$th Fibonacci number.

Our verification is a proof by induction: we use the recursion for the Fibonacci numbers to show that the formula (1) holds at every stage. The formula can be written as:

$$a_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$$

where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$. Now the reason it works is that $\alpha$ and $\beta$ have the following special property:

$$\begin{aligned}
\alpha^2 &= (\frac{1+\sqrt{5}}{2})^2 \\
&= \frac{(1+\sqrt{5})^2}{2^2} \\
&= \frac{1+2\sqrt{5}+(\sqrt{5})^2}{4} \\
&= \frac{1+2\sqrt{5}+5}{4} \\
&= \frac{6+2\sqrt{5}}{4} \\
&= \frac{3+\sqrt{5}}{2} \\
&= \frac{2}{2} + \frac{1+\sqrt{5}}{2} = 1+\alpha,
\end{aligned}$$

while

$$\begin{aligned}
\beta^2 &= (\frac{1-\sqrt{5}}{2})^2 \\
&= \frac{(1-\sqrt{5})^2}{2^2} \\
&= \frac{1-2\sqrt{5}+(\sqrt{5})^2}{4} \\
&= \frac{1-2\sqrt{5}+5}{4} \\
&= \frac{6-2\sqrt{5}}{4} \\
&= \frac{3-\sqrt{5}}{2} \\
&= \frac{2}{2} + \frac{1-\sqrt{5}}{2} = 1+\beta.
\end{aligned}$$

Now we can look at the things we're trying to prove:

$$a_n = \tfrac{1}{\sqrt{5}}(\alpha^n - \beta^n) \qquad \mathrm{P}(n)$$

**Base step** P(0) says

$$a_0 = \frac{1}{\sqrt{5}}\alpha^0 - \beta^0$$

which is true, because

$$\frac{1}{\sqrt{5}}(\alpha^0 - \beta^0) = \frac{1}{\sqrt{5}}(1-1) = 0 = a_0.$$

P(1) says

$$a_1 = \frac{1}{\sqrt{5}}\alpha^1 - \beta^1$$

which is true, because

$$\begin{aligned}
\frac{1}{\sqrt{5}}(\alpha^1 - \beta^1) &= \frac{\alpha - \beta}{\sqrt{5}} \\
&= \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}} \\
&= \frac{(1+\sqrt{5}) - (1-\sqrt{5})}{2\sqrt{5}} \\
&= \frac{1+\sqrt{5}-1+\sqrt{5}}{2\sqrt{5}} \\
&= \frac{2\sqrt{5}}{2\sqrt{5}} = 1 = a_1.
\end{aligned}$$

**Inductive step** Assuming that $\mathrm{P}(k-1)$ and $\mathrm{P}(k-2)$ are true, we set out to prove $\mathrm{P}(k)$, that is, that $a_k = \frac{1}{\sqrt{5}}(\alpha^k - \beta^k)$. Now our defining formula for $a_k$ says that it's $a_{k-1} + a_{k-2}$, so

$$\begin{aligned}
a_k &= a_{k-1} + a_{k-2} \\
&= \frac{1}{\sqrt{5}}(\alpha^{k-1} - \beta^{k-1}) + \frac{1}{\sqrt{5}}(\alpha^{k-2} - \beta^{k-2})
\end{aligned}$$

(because $\mathrm{P}(k-1)$ and $\mathrm{P}(k-2)$ are both supposed to be true)

$$\begin{aligned}
&= \frac{1}{\sqrt{5}}(\alpha^{k-1} - \beta^{k-1} + \alpha^{k-2} - \beta^{k-2}) \\
&= \frac{1}{\sqrt{5}}(\alpha^{k-1} + \alpha^{k-2} - (\beta^{k-1} + \beta^{k-2})) \\
&= \frac{1}{\sqrt{5}}(\alpha^{k-2}(\alpha+1) - \beta^{k-2}(\beta+1)) \\
&= \frac{1}{\sqrt{5}}(\alpha^{k-2}\alpha^2 - \beta^{k-2}\beta^2)
\end{aligned}$$

(because $\alpha^2 = \alpha + 1$, $\beta^2 = \beta + 1$)

$$= \frac{1}{\sqrt{5}}(\alpha^k - \beta^k),$$

and $a_k = \frac{1}{\sqrt{5}}(\alpha^k - \beta^k)$, which is what we needed to prove. This works for every $k \geq 2$, so the induction continues.

I hope you noticed that I was using a slightly different kind of induction here. Instead of saying

P(0) is true and $\mathrm{P}(k+1)$ is true whenever $\mathrm{P}(k)$ is true, so $\mathrm{P}(n)$ must be true for all $n \geq 0$,

I said

> P(0) and P(1) are true and P($k$) is true whenever P($k-1$) and P($k-2$) are both true, so P($n$) must be true for all $n \geq 0$.

This is still OK, because we can still work up the ladder:

> P(0) is true,
> P(1) is true,
> because P(0) and P(1) are both true, P(2) is true,
> because P(1) and P(2) are both true, P(3) is true,
> because P(2) and P(3) are both true, P(4) is true,
> because P(3) and P(4) are both true, P(5) is true,
> because P(4) and P(5) are both true, P(6) is true,
> $\ldots$;

the process still takes us as far as we like. If you think of induction as climbing a ladder, the *base step* is a machine to get you onto the bottom rung, and the *inductive step* is a machine to lift you from one rung to the next. To use the First Principle of Induction we need a proof that P($k$)$\Rightarrow$P($k+1$); that is, a machine which will lift us from level $k$ to level $k+1$. In the argument just above, the machine needed to rest on both the preceding levels; it was a proof that P($k-2$) and P($k-1$) together implied P($k$). So of course the base step had to check both P(0) and P(1), because our machine couldn't lift us from level 0 to level 1. But resting on levels 0 and 1, it could raise us to level 2; resting on levels 1 and 2, it could raise us to level 3; and so on. It would still take us to any point we needed to reach.

Now if you think about it, an inductive argument can use much more elaborate machinery if that seems to help. The point about a proof by induction is that we look at the propositions P(0), P(1), P(2), $\ldots$ in order, and don't even think about proving P(7) until we've done all the preceding ones. So (if it seems to be useful) when designing the machine to reach level $k$, we can assume that P($i$) is true for every $i < k$ – P($k-1$), P($k-2$), P($k-3$), P($k-4$), $\ldots$ all the way down to P(0) if we need to.

Putting this a little more formally, we have the

**Second Principle of Induction** or **Principle of Strong Mathematical Induction** Suppose we have a sequence of propositions, $P(0), P(1), \cdots, P(n), \cdots$. Suppose that $P(0)$ is true and that if $k > 0$ and $P(i)$ is true whenever $0 \leq i < k$ then $P(k)$ is true. Then $P(n)$ is true for all values of $n$.

In a sense, the Second Principle of Induction is more powerful than the First. Because if we know that P($k-1$) by itself implies P($k$), which is what we need if we're going to use the First Principle, then obviously P(0), P(1), $\ldots$, P($k-1$) all together will imply P($k$). So any proof which works for the First Principle will also work for the Second Principle. But in practice one quite often tries first for a proof using the First Principle *just because there are fewer such proofs.* Looking for a proof is like looking for anything else. If you are looking for a needle in a haystack, it's often sense to look in the smallest bale of hay first, not because you especially believe the needle's there, but because if it is there you're less likely to miss it just through being overwhelmed by the sheer quantity of stuff to sift through.

For an example of a proof where the Second Principle really is the easy one to use, try the following. Recall that a positive integer $p \geq 2$ is called *prime* if and only if $p$ can*not* be expressed as a product of two smaller positive numbers[18]. The first few primes are 2, 3, 5, 7, 11, 13, 17, $\ldots$[19]. For example 23 is prime but 51 is not, because $51 = 3 \times 17$.

**Example 17.1** Every integer $n \geq 2$ is either a prime or is a product of primes.
**Proof** The statement is

$$\text{either } n \text{ is a prime or } n \text{ is a product of primes} \qquad P(\text{n})$$

**Base step** P(2) says

$$\text{either 2 is a prime or 2 is a product of primes,}$$

[18] Some people say that 1 is a prime. But most mathematicians don't. 1 is special.
[19] 2 is the only even prime. That makes it the oddest of all the primes.

which is true, because 2 is a prime.

**Inductive step** Assume that $k > 2$ and that $\mathrm{P}(i)$ is true whenever $2 \le i < k$. We want to prove that

either $k$ is a prime or $k$ is a product of primes.

Well: if $k$ is a prime, this is certainly true. If it isn't, then it's equal to $i \times j$ where both $i$ and $j$ are less than $k$. Neither $i$ nor $j$ can be 1 (since then the other would have to be $k$), so both are between 2 and $k-1$, and both $\mathrm{P}(i)$ and $\mathrm{P}(j)$ are true; that is, $i$ and $j$ are either primes or products of primes. We can express them as

$$i = p_1 \times p_2 \times \ldots \times p_r, \quad j = q_1 \times q_2 \times \ldots \times q_s$$

where $p_1, p_2, \ldots, p_r, q_1, \ldots, q_s$ are all primes. (If $i$ is prime, we just take $r = 1$, $p_1 = i$.) So $k = i \times j = p_1 \times \ldots \times p_r \times q_1 \times \ldots \times q_s$ is also a product of primes. Since this works for any $k > 2$, $\mathrm{P}(n)$ is true for every $n \ge 2$.

For another example of the use of the Second Principle of Induction, I take another fundamental fact about whole numbers.

**Theorem** If $p$, $q \in \mathbb{P}$, there are $r$, $s \in \mathbb{Z}$ such that $rp + sq$ is a factor of both $p$ and $q$.

**proof** Actually the first question to sort out here is: what are we supposed to induce *on*? Both the First and Second principles insist on starting with a proposition of the form $\mathrm{P}(n)$. Here we have one which talks about two integers $p$ and $q$. Will it work if we call one of them $n$? is there anything else we can do?

There is a fairly standard approach to this. The idea of proofs by induction is that you do the 'smallest' numbers first. So presumably we should start with the cases $(p, q) = (1, 1)$, $(1, 2)$, $(2, 1)$, $(2, 2)$, $(1, 3)$, $(3, 1)$ (or perhaps $(1, 3)$ should come before $(2, 2)$). What we mean by saying that 'the pair $p$, $q$ is small' might be something like '$p + q$ is small' or 'the larger of $p$ and $q$ is small'. Actually it very often doesn't matter which of these rules we take; but my own prejudice is in favour of taking 'the larger of $p$ and $q$' as my measure of the size of the problem.

So let us try, for the statement $\mathrm{P}(n)$, the statement

> if $p$, $q \in \mathbb{P}$ and $\max(p, q) = n$, then there are integers $r$ and $s$ such that $rp + sq$ is a factor of both $p$ and $q$,

and see how we get on[20].

**Base step** If $n = 1$, then $\mathrm{P}(1)$ is

> if $p$, $q \in \mathbb{P}$ and $\max(p, q) = 1$, then there are integers $r$ and $s$ such that $rp + sq$ is a factor of both $p$ and $q$,

But this is certainly true, because if $\max(p, q) = 1$ then we can only have $p = q = 1$, in which case we can set $r = 1$, $s = 0$ and get $rp + sq = 1$, which is surely a factor of both $p$ and $q$.[21]

**Inductive step** Now suppose that $k > 1$, that $P(i)$ is true whenever $1 \le i < k$, and try to prove $\mathrm{P}(k)$:

> if $p$, $q \in \mathbb{P}$ and $\max(p, q) = k$, then there are integers $r$ and $s$ such that $rp + sq$ is a factor of both $p$ and $q$.

Let $p$, $q \in \mathbb{P}$ be such that $\max(p, q) = k$. We have to consider separately the three cases $p < q$, $p = q$ and $p > q$. The middle one is the simplest, so let's take that first:

> **case 1** If $p = q$, then set $r = 1$, $s = 0$, so that $rp + js = p$ is a factor of both $p$ and $q$ (just as in the case $p = q = 1$).

The other cases are virtually identical to each other. Let's take

> **case 2** If $p < q$, then $q = k$ and $1 \le p < k$, $1 \le q - p < k$, so $i = \max(p, q - p) < k$ and (by the inductive hypothesis) $\mathrm{P}(i)$ is true. So there are integers $r'$, $s$ such that $j = r'p + s(q - p)$ is a factor of both $p$ and $q - p$. But this means that $j$ is also a factor of $q$; while if we set $r = r' - s$, then $r$ is an integer and $j = rp + sq$. So we have found integers $r$ and $s$ such that $rp + sq$ is a factor of both $p$ and $q$, which is what we needed.

Finally,

[20] For the rest of this argument, I will write '$\max(p, q)$' for 'the larger of $p$ and $q$'; if $p = q$, then $\max(p, q) = p = q$.

[21] You will see that I am starting from the case $n = 1$ rather than the case $n = 0$. Actually $P(0)$ is easier, because there are *no* $p$, $q \in \mathbb{P}$ such that $\max(p, q) = 0$! so there is nothing to check.

**case 3** If $q < p$, then applying $\mathrm{P}(i)$ where $i = \max(p-q, q)$ we find $r,\ s' \in \mathbb{Z}$ such that $r(p-q) + s'q$ is a factor of both $p-q$ and $q$, in which case $rp + (s'-r)q$ is a factor of both $p$ and $q$.

Thus we have the result we need in all three cases, and the induction continues.

(This theorem underlies an extraordinary range of things. At the most elementary level, it means that if we take distinct prime numbers – say 13 and 23 – there will be integers $r$ and $s$ such that $13r + 23s = 1$. Of course one of $r$, $s$ will have to be positive and the other negative. Can you find such numbers?)

**Sums of reciprocals** The following is another interesting example of the use of the Second Principle of Induction, as well as being a very pretty fact.

**Theorem** Any rational number strictly between 0 and 1 can be expressed as a sum $\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} + \ldots + \frac{1}{m_r}$, where $r \geq 1$ and $m_1, \ldots, m_r$ are distinct integers greater than 0.

**proof** What makes this proof tricky is the fact that it's not at all clear what we should try to induce on. We are trying to prove something about fractions $\frac{p}{q}$, where $p,\ q \in \mathbb{P}$; should we try to induce on $p$, or $q$, or $p+q$, or what? It turns out that we can do it by inducing on the numerator $p$, letting the denominator look after itself, as follows.

Take for the inductive hypothesis the sentence

whenever $m > k$ the fraction $\frac{k}{m}$ can be expressed as $\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} + \ldots + \frac{1}{m_r}$, where $r \geq 1$ and $m_1, \ldots, m_r$ are distinct integers greater than 0. $\qquad \mathrm{P}(k)$

The start is now very easy.

**Base step** $\mathrm{P}(1)$ says just that

whenever $m > 1$ the fraction $\frac{1}{m}$ can be expressed as $\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} + \ldots + \frac{1}{m_r}$, where $r \geq 1$ and $m_1, \ldots, m_r$ are distinct integers greater than 0,

and this is certainly OK; all we have to do is to take $r = 1$ and $m_1 = m$, and we just have $\frac{1}{m} = \frac{1}{m}$, which is true.

The interesting part is in the

**Inductive step** Suppose that $k > 1$ and that $\mathrm{P}(i)$ is true whenever $1 \leq i < k$; we want to prove $\mathrm{P}(k)$. So take any $m > k$ and consider the fraction $\frac{k}{m}$. Where can we start? The key is: *be greedy.* We want to find some numbers adding up to $\frac{k}{m}$; well, start with the biggest number we're allowed. It's got to be a reciprocal $\frac{1}{m_1}$; now you make this big by making $m_1$ small, so the rule is

take the smallest $m_1$ such that $\frac{1}{m_1} \leq \frac{k}{m}$.

Now what do we know about $m_1$? First, we have $\frac{1}{m_1} \leq \frac{k}{m}$, so $m \leq km_1$. On the other hand, we know that we weren't allowed to use $m_1 - 1$, so $\frac{1}{m_1 - 1} > \frac{k}{m}$, and $m > km_1 - k$.

Now look at what's left. We have

$$\frac{k}{m} - \frac{1}{m_1} = \frac{km_1 - m}{mm_1}.$$

In this fraction, the denominator has got worse ($mm_1$ is going to be bigger than $m$), but the numerator is $km_1 - m$, and we know enough to locate this. Since $km_1 - k < m \leq km_1$,

$$-km_1 \leq -m < k - km_1, \quad km_1 - km_1 \leq km_1 - m < k.$$

Now if $km_1 - m = 0$ this is because $\frac{k}{m} = \frac{1}{m_1}$, and we're home. If $1 \leq km_1 - m < k$ then the inductive hypothesis tells us that $\mathrm{P}(km_1 - m)$ is true, so that $\frac{km_1 - m}{mm_1}$ is a sum of distinct reciprocals $\frac{1}{m_2} + \ldots + \frac{1}{m_r}$

say, and $\frac{k}{m} = \frac{1}{m_1} + \frac{1}{m_2} + \ldots + \frac{1}{m_r}$.

We haven't quite finished, because the point of this theorem is that we are expressing numbers as the sum of *distinct* reciprocals, and the inductive hypothesis tells us that $m_2, \ldots, m_r$ are all different, but doesn't say anything about $m_1$. However, the check that $m_1$ is different from the others is easy. We know that $\frac{1}{m_1} \leq \frac{k}{m} < \frac{1}{m_1 - 1}$. But this means that, for any $j \geq 2$,

$$\frac{1}{m_j} \leq \frac{k}{m} - \frac{1}{m_1} < \frac{1}{m_1 - 1} - \frac{1}{m_1} \leq \frac{2}{m_1} - \frac{1}{m_1} = \frac{1}{m_1},$$

because of course $m_1 - 1 \geq \frac{m_1}{2}$. (I suppose I ought to remark here that because $\frac{1}{m_1} \leq \frac{k}{m} < 1$, $m_1 \geq 2$.) So $\frac{1}{m_j} < \frac{1}{m_1}$ for every $j > 1$, and all the $m_j$ are different from $m_1$ as well as from each other.

Thus we can express $\frac{k}{m}$ as a sum of distinct reciprocals. As $m$ is arbitrary, $\mathrm{P}(k)$ is true and the induction proceeds.

**Appendix** (with some repetitions)

Version of 18.12.01

Recall the definition of the Fibonacci sequence:

$$a_0 = 0,\ a_1 = 1,\ a_n = a_{n-1} + a_{n-2} \text{ for every } n \geq 2.$$

Surprisingly, we have a straightforward formula:

$$a_n = \frac{1}{\sqrt{5}}\left( (\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n \right)$$

(What is surprising about this is that all the $\sqrt{5}$s somehow cancel out to give integer values for every $n$.) To check this, express the formula as

$$a_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$$

where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$. Now the reason it works is that $\alpha$ and $\beta$ have the following special property:

$$\begin{aligned}
\alpha^2 &= (\frac{1+\sqrt{5}}{2})^2 \\
&= \frac{1+2\sqrt{5}+5}{4} \\
&= \frac{4+2(1+\sqrt{5})}{4} = 1+\alpha,
\end{aligned}$$

while

$$\begin{aligned}
\alpha^2 &= (\frac{1-\sqrt{5}}{2})^2 \\
&= \frac{1-2\sqrt{5}+5}{4} \\
&= \frac{4-2(1+\sqrt{5})}{4} = 1+\beta,
\end{aligned}$$

Now we can look at the things we're trying to prove:

$$a_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n) \qquad \mathrm{P}(n)$$

**Base step** P(0) says

$$a_0 = \frac{1}{\sqrt{5}}\alpha^0 - \beta^0$$

which is true, because

$$\frac{1}{\sqrt{5}}(\alpha^0 - \beta^0) = \frac{1}{\sqrt{5}}(1-1) = 0 = a_0.$$

P(1) says

$$a_1 = \frac{1}{\sqrt{5}}(\alpha^1 - \beta^1)$$

which is true, because

$$
\begin{aligned}
\frac{1}{\sqrt{5}}(\alpha^1 - \beta^1) &= \frac{\alpha - \beta}{\sqrt{5}} \\
&= \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}} \\
&= \frac{2\sqrt{5}}{2\sqrt{5}} = 1 = a_1.
\end{aligned}
$$

**Inductive step** Assuming that $\mathrm{P}(n-1)$ and $\mathrm{P}(n-2)$ are true, we set out to prove $\mathrm{P}(n)$, that is, that $a_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n)$. Now our defining formula for $a_n$ says that it's $a_{n-1} + a_{n-2}$, so

$$
\begin{aligned}
a_n &= a_{n-1} + a_{n-2} \\
&= \tfrac{1}{\sqrt{5}}(\alpha^{n-1} - \beta^{n-1}) + \tfrac{1}{\sqrt{5}}(\alpha^{n-2} - \beta^{n-2})
\end{aligned}
$$

(because $\mathrm{P}(n-1)$ and $\mathrm{P}(n-2)$ are both supposed to be true)

$$
\begin{aligned}
&= \tfrac{1}{\sqrt{5}}(\alpha^{n-1} - \beta^{n-1} + \alpha^{n-2} - \beta^{n-2}) \\
&= \tfrac{1}{\sqrt{5}}(\alpha^{n-1} + \alpha^{n-2} - (\beta^{n-1} + \beta^{n-2})) \\
&= \tfrac{1}{\sqrt{5}}(\alpha^{n-2}(\alpha + 1) - \beta^{n-2}(\beta + 1)) \\
&= \tfrac{1}{\sqrt{5}}(\alpha^{n-2}\alpha^2 - \beta^{n-2}\beta^2)
\end{aligned}
$$

(because $\alpha^2 = \alpha + 1$, $\beta^2 = \beta + 1$)

$$
= \tfrac{1}{\sqrt{5}}(\alpha^n - \beta^n),
$$

and $a_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n)$, which is what we needed to prove. This works for every $n \geq 2$, so the induction continues.

I hope you noticed that I was using a slightly different kind of induction here. Instead of saying

P(0) is true and $\mathrm{P}(n+1)$ is true whenever $\mathrm{P}(n)$ is true, so $\mathrm{P}(n)$ must be true for all $n \geq 0$,

I said

P(0) and P(1) are true and $\mathrm{P}(n)$ is true whenever $\mathrm{P}(n-1)$ and $\mathrm{P}(n-2)$ are both true, so $\mathrm{P}(n)$ must be true for all $n \geq 0$.

This is still OK, because we can still work up the ladder:

P(0) is true,
P(1) is true,
because P(0) and P(1) are both true, P(2) is true,
because P(1) and P(2) are both true, P(3) is true,
because P(2) and P(3) are both true, P(4) is true,
because P(3) and P(4) are both true, P(5) is true,
because P(4) and P(5) are both true, P(6) is true,
. . . ;

the process still takes us as far as we like. If you think of induction as climbing a ladder, the *base step* is a machine to get you onto the bottom rung, and the *inductive step* is a machine to lift you from one rung to the next. To use the First Principle of Induction we need a proof that $\mathrm{P}(n) \Rightarrow \mathrm{P}(n+1)$; that is, a machine which will lift us from level $n$ to level $n+1$. In the argument just above, the machine needed to rest on both the preceding levels; it was a proof that $\mathrm{P}(n-2)$ and $\mathrm{P}(n-1)$ together implied $\mathrm{P}(n)$. So of course the base step had to check both P(0) and P(1), because our machine couldn't lift us from level 0 to level 1. But resting on levels 0 and 1, it could raise us to level 2; resting on levels 1 and 2, it could raise us to level 3; and so on. It would still take us to any point we needed to reach.

Now if you think about it, an inductive argument can use much more elaborate machinery if that seems to help. The point about a proof by induction is that we look at the propositions P(0), P(1), P(2), ... in order, and don't even think about proving P(7) until we've done all the preceding ones. So (if it seems to be useful) when designing the machine to reach level $n$, we can assume that P($i$) is true for every $i < n$ – P($n-1$), P($n-2$), P($n-3$), P($n-4$), ... all the way down to P(0) if we need to.

Putting this a little more formally, we have the

**Second Principle of Induction** or **Principle of Strong Mathematical Induction** Suppose we have a sequence of propositions, $P(0), P(1), \cdots, P(n), \cdots$. Suppose that $P(0)$ is true and that if $n > 0$ and $P(i)$ is true whenever $0 \leq i < n$ then $P(n)$ is true. Then $P(n)$ is true for every integer $n \geq 0$.

In a sense, the Second Principle of Induction is more powerful than the First. Because if we know that P($n-1$) by itself implies P($n$), which is what we need if we're going to use the First Principle, then obviously P(0), P(1), ..., P($n-1$) all together will imply P($n$). So any proof which works for the First Principle will also work for the Second Principle. But in practice one quite often tries first for a proof using the First Principle *just because there are fewer such proofs*. Looking for a proof is like looking for anything else. If you are looking for a needle in a haystack, it's often sense to look in the smallest bale of hay first, not because you especially believe the needle's there, but because if it is there you're less likely to miss it just through being overwhelmed by the sheer quantity of stuff to sift through.

For an example of a proof where the Second Principle really is the easy one to use, try the following. Recall that a positive integer $p \geq 2$ is called *prime* if and only if $p$ can*not* be expressed as a product of two smaller positive numbers[22]. The first few primes are 2, 3, 5, 7, 11, 13, 17, ...[23]. For example 23 is prime but 51 is not, because $51 = 3 \times 17$.

**Example 17.1** Every integer $n \geq 2$ is either a prime or is a product of primes.
**Proof** The statement is

$$\text{either } n \text{ is a prime or } n \text{ is a product of primes} \qquad P(\mathrm{n})$$

**Base step** P(2) says

either 2 is a prime or 2 is a product of primes,

which is true, because 2 is a prime.

**Inductive step** Assume that $k > 2$ and that P($i$) is true whenever $2 \leq i < k$. We want to prove that

either $k$ is a prime or $k$ is a product of primes.

Well: if $k$ is a prime, this is certainly true. If it isn't, then it's equal to $i \times j$ where both $i$ and $j$ are less than $k$. Neither $i$ nor $j$ can be 1 (since then the other would have to be $k$), so both are between 2 and $k-1$, and both P($i$) and P($j$) are true; that is, $i$ and $j$ are either primes or products of primes. We can express them as

$$i = p_1 \times p_2 \times \ldots \times p_r, \quad j = q_1 \times q_2 \times \ldots \times q_s$$

where $p_1, p_2, \ldots, p_r, q_1, \ldots, q_s$ are all primes. (If $i$ is prime, we just take $r = 1$, $p_1 = i$.) So $k = i \times j = p_1 \times \ldots \times p_r \times q_1 \times \ldots \times q_s$ is also a product of primes. Since this works for any $k > 2$, P($n$) is true for every $n \geq 2$.

For another example of the use of the Second Principle of Induction, I take another fundamental fact about whole numbers.

**Theorem** If $p$, $q \in \mathbb{P}$, there are $r$, $s \in \mathbb{Z}$ such that $rp + sq$ is a factor of both $p$ and $q$.

[22]Some people say that 1 is a prime. But most mathematicians don't. 1 is special.
[23]2 is the only even prime. That makes it the oddest of all the primes.

**proof** Actually the first question to sort out here is: what are we supposed to induce *on*? Both the First and Second principles insist on starting with a proposition of the form $\mathrm{P}(n)$. Here we have one which talks about two integers $p$ and $q$. Will it work if we call one of them $n$? is there anything else we can do?

There is a fairly standard approach to this. The idea of proofs by induction is that you do the 'smallest' numbers first. So presumably we should start with the cases $(p, q) = (1,1)$, $(1,2)$, $(2,1)$, $(2,2)$, $(1,3)$, $(3,1)$ (or perhaps $(1,3)$ should come before $(2,2)$). What we mean by saying that 'the pair $p$, $q$ is small' might be something like '$p+q$ is small' or 'the larger of $p$ and $q$ is small'. Actually it very often doesn't matter which of these rules we take; but my own prejudice is in favour of taking 'the larger of $p$ and $q$' as my measure of the size of the problem.

So let us try, for the statement $\mathrm{P}(n)$, the statement

> if $p$, $q \in \mathbb{P}$ and $\max(p, q) = n$, then there are integers $r$ and $s$ such that $rp + sq$ is a factor of both $p$ and $q$,

and see how we get on[24].

**Base step** If $n = 1$, then $\mathrm{P}(1)$ is

> if $p$, $q \in \mathbb{P}$ and $\max(p, q) = 1$, then there are integers $r$ and $s$ such that $rp + sq$ is a factor of both $p$ and $q$,

But this is certainly true, because if $\max(p, q) = 1$ then we can only have $p = q = 1$, in which case we can set $r = 1$, $s = 0$ and get $rp + sq = 1$, which is surely a factor of both $p$ and $q$. (You will see that I am starting from the case $n = 1$ rather than the case $n = 0$. Actually $P(0)$ is easier, because there are *no* $p$, $q \in \mathbb{P}$ such that $\max(p, q) = 0$! so there is nothing to check.)

**Inductive step** Now suppose that $k > 1$, that $P(i)$ is true whenever $1 \leq i < k$, and try to prove $\mathrm{P}(k)$:

> if $p$, $q \in \mathbb{P}$ and $\max(p, q) = k$, then there are integers $r$ and $s$ such that $rp + sq$ is a factor of both $p$ and $q$.

Let $p$, $q \in \mathbb{P}$ be such that $\max(p, q) = k$. We have to consider separately the three cases $p < q$, $p = q$ and $p > q$. The middle one is the simplest, so let's take that first:

> **case 1** If $p = q$, then set $r = 1$, $s = 0$, so that $rp + js = p$ is a factor of both $p$ and $q$ (just as in the case $p = q = 1$).

The other cases are virtually identical to each other. Let's take

> **case 2** If $p < q$, then $q = k$ and $1 \leq p < k$, $1 \leq q - p < k$, so $i = \max(p, q - p) < k$ and (by the inductive hypothesis) $\mathrm{P}(i)$ is true. So there are integers $r'$, $s$ such that $j = r'p + s(q - p)$ is a factor of both $p$ and $q - p$. But this means that $j$ is also a factor of $q$; while if we set $r = r' - s$, then $r$ is an integer and $j = rp + sq$. So we have found integers $r$ and $s$ such that $rp + sq$ is a factor of both $p$ and $q$, which is what we needed.

Finally,

> **case 3** If $q < p$, then applying $\mathrm{P}(i)$ where $i = \max(p - q, q)$ we find $r$, $s' \in \mathbb{Z}$ such that $r(p - q) + s'q$ is a factor of both $p - q$ and $q$, in which case $rp + (s' - r)q$ is a factor of both $p$ and $q$.

Thus we have the result we need in all three cases, and the induction continues.

(This theorem underlies an extraordinary range of things. At the most elementary level, it means that if we take distinct prime numbers – say 13 and 23 – there will be integers $r$ and $s$ such that $13r + 23s = 1$. Of course one of $r$, $s$ will have to be positive and the other negative. Can you find such numbers?)

**Sums of reciprocals** The following is another interesting example of the use of the Second Principle of Induction, as well as being a very pretty fact.

**Theorem** Any rational number strictly between 0 and 1 can be expressed as a sum $\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} + \ldots + \frac{1}{m_r}$, where $r \geq 1$ and $m_1, \ldots, m_r$ are distinct integers greater than 0.

**proof** What makes this proof tricky is the fact that it's not at all clear what we should try to induce on. We are trying to prove something about fractions $\frac{p}{q}$, where $p$, $q \in \mathbb{N} \setminus \{0\}$; should we try to induce on $p$, or

---

[24] For the rest of this argument, I will write '$\max(p, q)$' for 'the larger of $p$ and $q$'; if $p = q$, then $\max(p, q) = p = q$.

$q$, or $p+q$, or what? It turns out that we can do it by inducing on the numerator $p$, letting the denominator look after itself, as follows.

Take for the inductive hypothesis the sentence

whenever $m > k$ the fraction $\frac{k}{m}$ can be expressed as $\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} + \ldots + \frac{1}{m_r}$, where $r \geq 1$ and $m_1, \ldots, m_r$ are distinct integers greater than 0. P($k$)

The start is now very easy.

**Base step** P(1) says just that

whenever $m > 1$ the fraction $\frac{1}{m}$ can be expressed as $\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} + \ldots + \frac{1}{m_r}$, where $r \geq 1$ and $m_1, \ldots, m_r$ are distinct integers greater than 0,

and this is certainly true; all we have to do is to take $r = 1$ and $m_1 = m$, and we just have $\frac{1}{m} = \frac{1}{m}$, which is true.

The interesting part is in the

**Inductive step** Suppose that $k > 1$ and that P($i$) is true whenever $1 \leq i < k$; we want to prove P($k$). So take any $m > k$ and consider the fraction $\frac{k}{m}$.

Where can we start? The key is: *be greedy.* We want to find some numbers adding up to $\frac{k}{m}$; well, start with the biggest number we're allowed. It's got to be a reciprocal $\frac{1}{m_1}$; now you make this big by making $m_1$ small, so the rule is

take the smallest $m_1$ such that $\frac{1}{m_1} \leq \frac{k}{m}$.

Now what do we know about $m_1$? First, we have $\frac{1}{m_1} \leq \frac{k}{m}$, so $m \leq km_1$. On the other hand, we know that we weren't allowed to use $m_1 - 1$, so $\frac{1}{m_1-1} > \frac{k}{m}$, and $m > km_1 - k$.

Now look at what's left. We have

$$\frac{k}{m} - \frac{1}{m_1} = \frac{km_1-m}{mm_1}.$$

In this fraction, the denominator has got worse ($mm_1$ is going to be bigger than $m$), but the numerator is $km_1 - m$, and we know enough to locate this. Since $km_1 - k < m \leq km_1$,

$$-km_1 \leq -m < k - km_1, \quad km_1 - km_1 \leq km_1 - m < k.$$

Now if $km_1 - m = 0$ this is because $\frac{k}{m} = \frac{1}{m_1}$, and we're home. If $1 \leq km_1 - m < k$ then the inductive hypothesis tells us that P($km_1 - m$) is true, so that $\frac{km_1-m}{mm_1}$ is a sum of distinct reciprocals $\frac{1}{m_2} + \ldots + \frac{1}{m_r}$ say, and $\frac{k}{m} = \frac{1}{m_1} + \frac{1}{m_2} + \ldots + \frac{1}{m_r}$.

We haven't quite finished, because the point of this theorem is that we are expressing numbers as the sum of *distinct* reciprocals, and the inductive hypothesis tells us that $m_2, \ldots, m_r$ are all different, but doesn't say anything about $m_1$. However, the check that $m_1$ is different from the others is easy. We know that $\frac{1}{m_1} \leq \frac{k}{m} < \frac{1}{m_1-1}$. But this means that, for any $j \geq 2$,

$$\frac{1}{m_j} \leq \frac{k}{m} - \frac{1}{m_1} < \frac{1}{m_1-1} - \frac{1}{m_1} \leq \frac{2}{m_1} - \frac{1}{m_1} = \frac{1}{m_1},$$

because of course $m_1 - 1 \geq \frac{m_1}{2}$. (I suppose I ought to remark here that because $\frac{1}{m_1} \leq \frac{k}{m} < 1$, $m_1 \geq 2$.) So $\frac{1}{m_j} < \frac{1}{m_1}$ for every $j > 1$, and all the $m_j$ are different from $m_1$ as well as from each other.

Thus we can express $\frac{k}{m}$ as a sum of distinct reciprocals. As $m$ is arbitrary, P($k$) is true and the induction proceeds.

**Remark** In fact we can do a bit better; the result is true for any rational number greater than 0, not just those between 0 and 1. To see this, we need to know the following, which is very important in itself.

**Theorem** For any $n \in \mathbb{N}$,

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots + \frac{1}{2^n} \geq 1 + \frac{n}{2}.$$

**proof** Induce on $n$, using the First Principle.
**Base step** If $n = 0$, then we are saying that

$$1 \geq 1 + \frac{0}{2},$$

which is certainly true.
**Inductive step** Assuming that

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{2^n} \geq 1 + \frac{n}{2}$$

we want to prove that

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{2^{n+1}} \geq 1 + \frac{n+1}{2}.$$

But

$$\begin{aligned} 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{2^{n+1}} &= 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{2^n} + \frac{1}{2^n+1} + \ldots \frac{1}{2^{n+1}} \\ &\geq 1 + \frac{n}{2} + \frac{1}{2^n+1} + \frac{1}{2^n+2} + \ldots + \frac{1}{2^{n+1}-1} + \frac{1}{2^{n+1}} \end{aligned}$$

(by the inductive hypothesis)

$$\geq 1 + \frac{n}{2} + \frac{1}{2^{n+1}} + \ldots \frac{1}{2^{n+1}}$$

(because $\frac{1}{k} \geq \frac{1}{2^{n+1}}$ whenever $2^n < k \leq 2^{n+1}$)

$$= 1 + \frac{n}{2} + \frac{2^n}{2^{n+1}}$$

(because there are just $2^n$ terms to be added up)

$$= 1 + \frac{n}{2} + \frac{1}{2} = 1 + \frac{n+1}{2}.$$

So the induction proceeds.

**Theorem** Every rational number greater than 0 can be expressed as a sum of distinct reciprocals.

**proof** Let $a > 0$ be rational. If $a < 1$ we already know that it can be expressed as a sum of distinct rationals. If $a \geq 1$, consider $1$, $1 + \frac{1}{2}$, $1 + \frac{1}{2} + \frac{1}{3}$, .... We know that eventually these sums have to go past $a$; if $n \geq 2(a-1)$, then

$$1 + \frac{1}{2} + \ldots + \frac{1}{2^n} \geq 1 + \frac{n}{2} \geq a.$$

So we must be able to find some $k$ such that

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{k} \leq a < 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{k} + \frac{1}{k+1}.$$

If $a = 1 + \frac{1}{2} + \ldots + \frac{1}{k}$ we can stop. Otherwise, set $b = a - 1 - \frac{1}{2} - \ldots - \frac{1}{k}$. Then $b$ is a rational number strictly between 0 and $\frac{1}{k+1}$. By the theorem above, we can express $b$ as $\frac{1}{m_1} + \ldots + \frac{1}{m_r}$ where $m_1, \ldots, m_r$ are all different, so that

$$a = 1 + \frac{1}{2} + \ldots + \frac{1}{k} + \frac{1}{m_1} + \ldots + \frac{1}{m_r}.$$

Also, for $1 \leq i \leq r$, $\frac{1}{m_i} \leq b < \frac{1}{k+1}$ so $m_i > k+1$; thus all the numbers $1, 2, \ldots, k, m_1, \ldots, m_r$ are different and we have expressed $a$ as a sum of distinct reciprocals.

**The Marriage Lemma** For my last example of a proof by induction, I will try to explain one of the most important theorems of 'combinatorics' – the branch of mathematics which deals with patterns and counting. First, a bit of special notation. If $R$ is a relation (that is, a set of ordered pairs), and $I$ is a set, I will write $R[I] = \{y : \exists\, x \in I,\, (x, y) \in R\}$ for the set of objects related to some member of $I$ by the relation $R$. Next, we need to know what an 'injective' function is. A function $f$ is **injective** or **one-to-one** if

it never takes the same value twice

the equation $f(x) = y$ never has more than one solution for $x$

if $x$, $x'$ are different points in the domain of $f$, then $f(x) \neq f(x')$

if $x$, $x' \in \operatorname{dom} f$ and $f(x) = f(x')$ then $x = x'$;

all these four expressions are supposed to be saying the same thing. In terms of the familiar functions of calculus,

$$f(x) = \exp x \text{ for } x \in \mathbb{R},$$

$$f(x) = \ln x \text{ for } x > 0,$$

$$f(x) = x^3 \text{ for } x \in \mathbb{R},$$

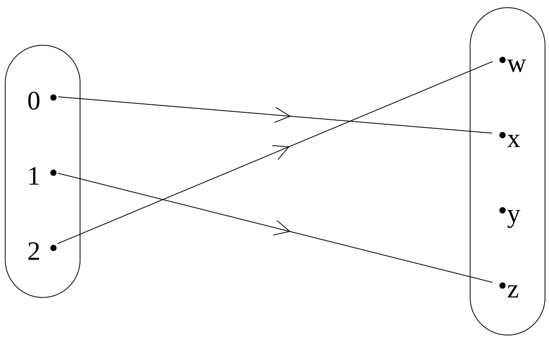
$$f(x) = \sqrt{x} \text{ for } x \geq 0$$

are all injective, but

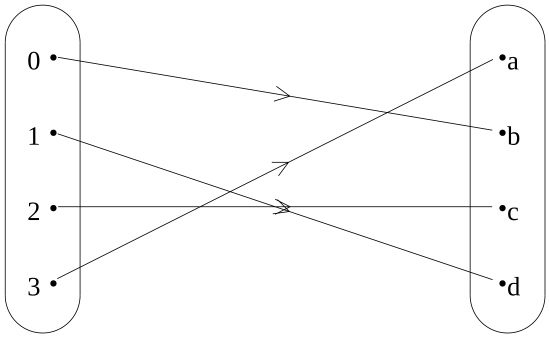
$$f(x) = x^2 \text{ for } x \in \mathbb{R},$$

$$f(x) = \sin x \text{ for } x \in \mathbb{R}$$

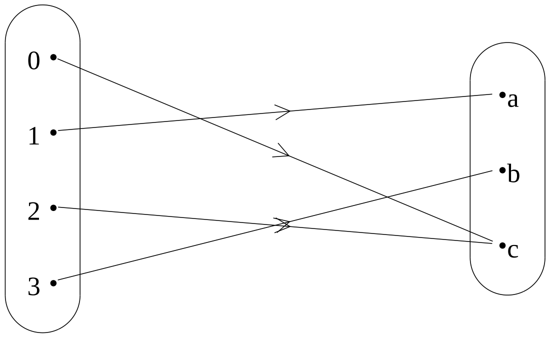
are not ($(-1)^2 = 1^2$, $\sin 0 = \sin \pi$). In terms of arrow diagrams,




and




represent injective functions, but




does not.

Now for the theorem.

**Hall's Marriage Lemma** Suppose that $X$ is a finite set, $Y$ is any set, and $R \subseteq X \times Y$ is a relation such that $\#(R[I]) \geq \#(I)$ for every $I \subseteq X$. Then there is an injective function $f : X \to Y$ such that $(x, f(x)) \in R$ for every $x \in X$.

**Remarks** Before starting on the proof, let me explain why this is called the 'marriage lemma'. Imagine that $X$ is a set of girls, $Y$ is a set of boys and that $R$ is the set of pairs $(x, y)$ who are willing to dance together. A master of ceremonies is trying to pair them off; that is, to find a function $f$ so that $f(x)$ will be the partner of $x$. Every girl is supposed to get a partner (that is, $\mathrm{dom}\, f$ should be $X$); every girl should have a different partner (that is, $f$ should be injective); and all pairs should be acceptable to each other (that is, $(x, f(x))$ should belong to $R$ for every $x$). The Marriage Lemma gives a rule to decide when there will be such a pairing.

Generally, the Marriage Lemma gives us a rule for deciding when allocation problems are soluble. For almost any kind of finite allocation of discrete objects it is the first thing to look at.

Proof of the Marriage Lemma Induce on $\#(X)$, using the Second Principle of Induction.

**Base step** If $\#(X) = 0$, that is, $X = \emptyset$, the problem is trivial. We have no girls to find partners for and don't have to do anything. Technically speaking, $R = \emptyset$ and the function $f$ will have to be the 'empty function', the function with domain $\emptyset$ and no values.

**Inductive step** Suppose that the lemma is true whenever $0 \leq \#(X) < n$, where $n > 0$, and that we are given $X$, $Y$ and $R$ such that $\#(X) = n$, $R \subseteq X \times Y$ and $\#(R[I]) \geq \#(I)$ for every $I \subseteq X$; we are looking for a suitable function from $X$ to $Y$.

**Case 1** Suppose that there is a set $I \subseteq X$ such that $0 < \#(I) < \#(X)$ and $\#(R[I]) = \#(I)$.
In this case, set

$$X_1 = I, \quad R_1 = R \cap (I \times Y),$$

$$X_2 = X \setminus I, \quad R_2 = R \cap ((X \setminus I) \times (Y \setminus R[I])).$$

Then $R_1 \subseteq X_1 \times Y$. If $J \subseteq X_1$, $R_1[J] = R[J]$ so $\#(R_1[J]) = \#(R[J]) \geq \#(J)$. Also $\#(X_1) < \#(X) = n$; by the inductive hypothesis, there is an injective function $f_1 : X_1 \to Y$ such that $(x, f_1(x)) \in R_1$ for every $x \in X_1$.

Next, $R_2 \subseteq X_2 \times Y$. If $J \subseteq X_2$, then

$$R_2[J] = R[J] \setminus R[I] = (R[I] \cup R[J]) \setminus R[I] = R[I \cup J] \setminus R[I],$$

so

$$\#(R_2[J]) = \#(R[I \cup J]) - \#(R[I]) \geq \#(I \cup J) - \#(I) = \#(I \cup J) - \#(I)$$

(by the choice of $I$)

$$= \#(J).$$

Also $\#(X_2) < \#(X) = n$; by the inductive hypothesis again, there is an injective function $f_2 : X_2 \to Y$ such that $(x, f_2(x)) \in R_2$ for every $x \in X_2$.

Now define $f : X \to Y$ by setting

$$\begin{aligned} f(x) &= f_1(x) \text{ if } x \in X_1 \\ &= f_2(x) \text{ if } x \in X_2. \end{aligned}$$

If $x \in X_1$, then

$$(x, f(x)) = (x, f_1(x)) \in R_1 \subseteq R;$$

if $x \in X_2$, then

$$(x, f(x)) = (x, f_2(x)) \in R_2 \subseteq R.$$

So $(x, f(x)) \in R$ for every $x \in X$. If $x$, $x' \in X$ are distinct, then

if $x$, $x' \in X_1$, $f(x) = f_1(x) \neq f_1(x') = f(x')$ because $f_1$ is injective,

if $x$, $x' \in X_2$, $f(x) = f_2(x) \neq f_2(x') = f(x')$ because $f_2$ is injective,

if $x \in X_1$ and $x' \in X_2$, $(x, f(x)) \in R$ and $x \in I$ so $f(x) \in R[I]$, while

$$(x', f(x')) = (x', f_2(x')) \in R_2 \subseteq (X \setminus I) \times (Y \setminus R[I])$$

so $f(x') \notin R[I]$, and $f(x')$ cannot be equal to $f(x)$,

if $x \in X_2$ and $x' \in X_1$ then $f(x') \in R[I]$ while $f(x) \notin R[I]$, so $f(x) \neq f(x')$.

Thus $f(x) \neq f(x')$ in all cases, and $f$ is injective. So we have a function of the kind we need, at least when there is an $I \subseteq X$, neither $\emptyset$ nor $X$, such that $\#(R[I]) = \#(I)$.

**Case 2** Suppose that $\#(R[I]) \neq \#(I)$ whenever $I \subseteq X$ and $0 < \#(I) < \#(X)$; that is, $\#(R[I]) > \#(I)$ for every such $I$. We are supposing that $\#(X) = n > 0$, so $X \neq \emptyset$; take any $x_0 \in X$. Since $\#(R[\{x_0\}]) \geq \#(\{x_0\}) = 1$, $R([\{x_0\}])$ is not empty; take any $y_0 \in R[\{x_0\}]$, so that $(x_0, y_0) \in R$.

Now set $X_1 = X \setminus \{x_0\}$ and set

$$R_1 = R \cap ((X \setminus \{x_0\}) \times (Y \setminus \{y_0\})).$$

Then $R_1 \subseteq X_1 \times Y$. If $J \subseteq X_1$ and $J \neq \emptyset$, then $0 < \#(J) < \#(X)$ so $\#(R[J]) > \#(J)$. But $R_1[J] \supseteq R[J] \setminus \{y_0\}$, so

$$\#(R_1[J]) \geq \#(R[J]) - 1 \geq \#(J).$$

If $J = \emptyset$ then of course $\#(R_1[J]) \geq 0 = \#(J)$. Also $\#(X_1) < \#(X) = n$. By the inductive hypothesis yet again, there is an injective function $f_1 : X \to Y$ such that $(x, f_1(x)) \in R_1$ for every $x \in X_1$.

Define $f : X \to Y$ by setting

$$\begin{aligned} f(x) &= y_0 \text{ if } x = x_0 \\ &= f_1(x) \text{ if } x \in X_1. \end{aligned}$$

If $x = x_0$, then

$$(x, f(x)) = (x_0, y_0) \in R;$$

if $x \in X_1$, then

$$(x, f(x)) = (x, f_1(x)) \in R_1 \subseteq R.$$

So $(x, f(x)) \in R$ for every $x \in X$. If $x$, $x' \in X$ are distinct, then
if $x$, $x' \in X_1$, $f(x) = f_1(x) \neq f_1(x') = f(x')$ because $f_1$ is injective,
if $x = x_0$ and $x' \in X_1$, $f(x_0) = y_0$, while

$$(x', f(x')) = (x', f_1(x')) \in R_1 \subseteq (X \setminus \{x_0\}) \times (Y \setminus \{y_0\}$$

so $f(x') \neq y_0$, and $f(x')$ cannot be equal to $f(x)$,
if $x \in X_1$ and $x' = x_0$ then $f(x') = y_0 \neq f(x)$.
Thus $f(x) \neq f(x')$ in all cases, and $f$ is injective. So we have a function of the kind we need in this case also.

Thus the induction proceeds.

**Remark** The above proof is complete and correct; I do not think it is 'easy', but I hope you can see the principle involved; if there is a critical set $I$ such that $R[I]$ is exactly the same size as $I$, then the whole of $R[I]$ will have to be used up in allocating the members of $I$, and the rest of $X$ will have to make do with members of $Y \setminus R[I]$; 'case 1' of the inductive step is just the check that in fact they will be able to manage. If there isn't a critical set, then we can get away with making the first assignment $f(x_0)$ without looking at anyone else, and the rest will again be able to make do with what's left.

I ought however to tell you that for many purposes this is not the 'best' proof. The trouble is that it gives you no indication of how to actually make the allocation. If $X$ has 1000 members, say, the proof seems to ask you to look at every one of the $2^{1000}$ subsets $I$ of $X$ to see if one of them has $\#(R[I]) = \#(I)$. This will forever be completely impracticable. There is however a quite different (and more difficult) proof of the theorem which provides an algorithm for finding the injective function which, on currently available computers, could be made to work so long as $\#(R)$ is not too enormous – $\#(R) = 10000$ shouldn't be beyond a fast PC with a patient customer.