ALGEBRA

Contents

1 Preamble: A brief intro to sets and numbers **5**

2 Sets **9**

2.1 Sets built from other sets 10

2.1.1 Subsets 10

2.1.2 Intersection and union 12

2.2 More Sets built from other sets 13

2.2.1 Cartesian product 14

2.2.2 Aside on the subsets of the set of real numbers 15

2.3 Relations and Functions 16

2.3.1 Functions 17

2.3.2 Injection and surjection 19

2.3.3 Composition of functions 20

2.4 Orderings 21

2.4.1 Diagrammatic representation of posets: Hasse diagrams 22

2.4.2 Structure of ordered sets 23

2.4.3 Ordinals 24

2.4.4 More on posets 25

2.5 Equivalence Relations 26

2.5.1 Equivalence classes 27

2.6 Countability 30

2.7 Permutations 34

3 Complex Numbers **37**

3.1 Polar representation and Argand diagram 39

4 Sequences and Series **43**

4.1 Summation of series 43

4.1.1 Generalities 43

4.1.2 Method of differences 44

4.2 Infinite Series 46

4.3 Introduction to difference equations 47

Chapter 1

Preamble: A brief intro to sets and numbers

We assume here that you are reasonably happy with the idea of a collection of "objects". This is a bit vague and potentially troublesome. But it *is* very useful, and we have to start somewhere. We will use the term 'set' for a collection of objects.

Suppose that we (you and I) both have in mind a set. Let's call it S. To say that we both have it is to say that we agree on what the "elements" are — the objects that are collected in S. Thus if we both have in mind an object x (say), we can agree if the statement 'x is in S' (written $x \in S$) is true or false (if false then we write $x \notin S$).

What might constitute a good "object"? In practice this is anything that we can agree is a good object. Just to get things started with a minimum of trouble, we can say that a set itself can be an object. Let us also say that there is one formal set, call it $\emptyset$, that does not contain any objects — thus postponing the general issue of what an object is by avoiding it. Thus the statement '$x \in \emptyset$' is false for every object x.

Putting these two ideas together, we have another set: the set containing only the set $\emptyset$.

If we have given a name to an object, like $\emptyset$, or X perhaps, then we can

write the set containing only that object as $\{X\}$. The only concrete example of this that we have so far is $\{\emptyset\}$. For this at least we can say $\emptyset \in \{\emptyset\}$ and $x \notin \{\emptyset\}$ for all other objects x.

We say that two sets are equal if they contain the same elements; and otherwise they are unequal. Thus $\emptyset \neq \{\emptyset\}$.

Suppose that x and y and z represent objects, somehow agreed between us. One way of writing that x and y and z are in S (that $x, y, z \in S$) is $S = \{x, y, z, ...\}$. Another way is $S = \{y, x, z, ...\}$. If x, y, z are the only elements in S then we can write $S = \{x, y, z\}$. The extension of this notation to more (or fewer) elements can be guessed. (For the moment the question of precisely what the objects x, y, z here are remains mysterious.)

And then, using this notation, another set with un-mysterious objects is $\{\emptyset, \{\emptyset\}\}$. Notice that this is not equal as a set either to $\emptyset$ or to $\{\emptyset\}$. And notice that we can 'iterate' this construction: the set containing all the sets we have so far as elements is a new set; and now we can make another new set by adding this new set as a new element.

With such unappealing constructions of new sets, and hence new objects, we can at least delay the discussion of more interesting (but maybe not clearly defined) objects. We do now have many objects available — just by iterating the construction of adding a new set to a set of sets.

One more device before we really get started. Suppose that a and b represent objects (not even necessarily distinct). An *ordered pair*, denoted (a, b), is a set $\{\{a\}, \{a, b\}\}$.
(Caveat: this notation (a, b) can be used in other contexts as well, to represent other things. So, to be safe, if we do mean it to denote an ordered pair then we will say so explicitly.)

Because of the way we write (and talk; and think) it sometimes looks like there is order in expressions like $\{a, b\}$ already. But note from above that $\{a, b\} = \{b, a\}$ so there is not. However note that $(a, b) \neq (b, a)$ (unless $a = b$) — this is a good exercise to prove.

Some further reading:

Beginning Finite Mathematics (Schaum's Outline Series), S Lipschutz et al.
Discrete Mathematics, J K Truss.
Sets, Logic and Categories, P J Cameron (Springer).
Algebra Volume 1, P M Cohn.

Chapter 2

Sets

- A SET is a collection of objects.
- A specific set is 'defined' by any means which unambiguously tells us how to determine whether an arbitrary object is in the set or not.
- The objects in a set are called the ELEMENTS of the set. We write $x \in S$ in case x is an element of set S. We write $x \notin S$ otherwise.

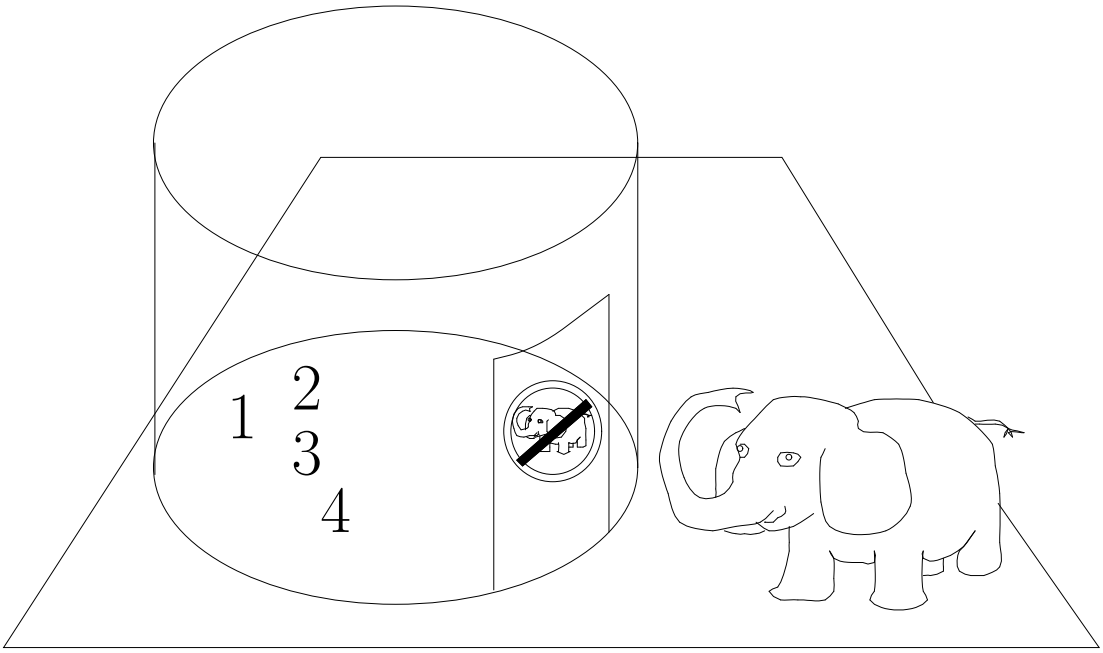
Example 1 *Suppose we write* $S = \{1, 2, 3, 4\}$. *Then* S *is a set,* $1 \in S$, *and* $2 \in S$, *but* $5 \notin S$, *and of course* $\boxed{[\mathfrak{My}\ \textit{pet ElephanT}]} \notin S$ *(see figure).*

Example 2 *Suppose* $T = \{x \text{ an integer} \mid x^2 < 27\}$. *This is another set (here* $\mid$ *means 'such that'; and we are assuming just for now that you know what 'integer' and* $<$ *mean). We have* $-1 \in T$, $6 \notin T$, $-6 \notin T$, $0 \in T$, *and so on.*

Example 3 *Suppose* $V = \{0, 1, 2, 3, 4, 5, -1, -2, -3, -4, -5\}$. *This is also a set. The order in which we write the elements in a set is not important.*

In general, the *language* of SET THEORY aims to be very precise.

Recall how computers refuse to try to understand even the slightest deviation from their computer languages. Although the language of set theory is intended to be read by humans, we are trying to achieve (almost) the same



level of discipline and precision as the computers, so we require almost the same level of discipline in our language.

This has the advantage that we less often confuse or mislead our audience, but the disadvantage that communication can seem slow, and hence sometimes boring.

If one does not value telling the truth, then set theory language will seem like a waste of time; but if one does value telling the truth, and hearing the truth, then it is a good idea to be patient with it! *Ultimately* it is rewarding.

2.1 Sets built from other sets

2.1.1 Subsets

Definition 2.1.[SUBSET] A set S is a subset of a set T if and only if every element of S is an element of T.

A *mathematical notation* representation of this definition is:

$$S \subseteq T \iff (x \in S \Rightarrow x \in T).$$

Make sure you understand what each symbol means, and how to read this line as a sentence in ordinary language! For example, $\subseteq$ is the symbol for subset; $\iff$, also written *iff*, means 'if and only if'; and $\Rightarrow$ is the symbol for 'implies'. The brackets here are a guide to the eye, containing a statement within the sentence which is a composite of other statements.

Example 4 *Comparing S from example 1 and T from example 2 we see that $S \subseteq T$.*

Example 5 *Let $\mathcal{S}$ be the set of playing cards in a 52 card deck of playing cards. Then the set of all 'club' cards is a subset $\mathcal{S}_\clubsuit$ of $\mathcal{S}$. Suppose that a card dealer deals out the pack into 4 equal hands (i.e. 13 cards each). Each of these hands is a subset of $\mathcal{S}$.* What is the probability that one of these hands is $\mathcal{S}_\clubsuit$?

A set $S \subseteq T$ is called a PROPER subset of T (in our notation this is written $S \subset T$) provided at least one element of T is not in S.

We write $S = T$ if $S \subseteq T$ and $T \subseteq S$.

Example 6 *Comparing T from example 2 and V from example 3 we see that $T = V$.*

Exercise 1 *Write down five sets — call them S_1, S_2, S_3, S_4, S_5, say — with the property that $S_i \subset S_{i+1}$ for $i = 1, 2, 3, 4$ (i.e. $S_1 \subset S_2$, and so on).*

Exercise 2 *Show that for A, B, C sets, if $A \subset B$ and $B \subset C$ then $A \subset C$.*

The general procedure for solving this kind of problem is as follows:

State what is to be done in mathematical notation; *if* the solution is very long (not the case here, as we will see!) give a one sentence overview of your plan of attack; convert the known information into mathematical notation (expanding up all terms to their full definitions) and rearrange to achieve the required result....

Solution 2.1 *We need to show that $x \in A$ implies $x \in C$, and that there is some $y \in C$ such that $y \notin A$. Suppose that $A \subset B$ and $B \subset C$. Since $A \subset B$ then $x \in A$ implies $x \in B$. Further since $B \subset C$ then $x \in B$ implies $x \in C$. Altogether then $x \in A$ implies $x \in C$, which shows that $A \subseteq C$. But $A \subset B$ also implies that there exists $y \in B$ such that $y \notin A$, and since $y \in B$ implies $y \in C$ then $A \subset C$. QED.*

2.1.2 Intersection and union

In what follows, S, T are two sets:

Definition 2.2.[INTERSECTION] We define a new set, the 'intersection of S and T', written $S \cap T$, by

$$S \cap T = \{x | x \in S \text{ and } x \in T\}.$$

For example, if $S = \{1, 2, 4\}, T = \{1, 3, 4, 5, 6\}$, then $S \cap T = \{1, 4\}$.
The EMPTY set, denoted $\emptyset$, is the set containing no objects. For example,

$$\{1, 3, 5\} \cap \{2, 4, 6\} = \emptyset.$$

Definition 2.3.[DISJOINT] We say that two sets A, B are disjoint in case $A \cap B = \emptyset$.

Example 7 *Let W be the set of all those ancient Egyptian pyramids under whose northernmost foundation stone is hidden evidence that aliens once visited the Earth. It is true to say that there is a set E such that $W \supseteq E$, since $W \supseteq \emptyset$ and $W \supseteq W$. But is it true that there is a set E such that $W \supset E$?*

Definition 2.4.[UNION] We define a new set

$$S \cup T = \{x | x \in S \text{ or } x \in T\}.$$

N.B. The 'or' here is the *inclusive or*.
For example, if $S = \{1, 2, 4\}, T = \{1, 3, 4, 5, 6\}$, then $S \cup T = \{1, 2, 3, 4, 5, 6\}$.

Exercise 3 *Verify that* $S \cup (T \cup V) = (S \cup T) \cup V$ *for all sets* S, T, V.

From this exercise we see that we may speak unambiguously of the union of several sets (i.e. not just two sets).

2.2 More Sets built from other sets

Definition 2.5.[POWER SET] The power set of a set S, denoted $\mathcal{P}(S)$, is the set of all subsets of S.

Example 8 $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$. *Notice how careful one must be with the brackets for this to make any sense.*

Every year, one of the things which people find confusing about algebra is the DEFINITIONS. It is completely normal to have trouble understanding a definition. But the definitions are crucial, so we must work to understand them. Let us try to use the definition above to illustrate how to read a definition in general — we might call this examining THE ANATOMY OF A DEFINITION.

The definition above is the definition of the term *Power set*. In other words it is a precise statement of what this term means, i.e. what it takes to qualify to be a power set. All definitions of terms are written using *other* terms. These other terms have either already been defined, or else their meaning has otherwise already been agreed. In theory this means we only *use* terms which we have already understood.

Thus the first thing to do in trying to understand a new definition is to check if we understand all the 'old' terms used in it. If there are any of these which we do not understand then we should transfer our attention to trying to understand them *first*. Since (I claim) no sequence of definitions is circular, this process will eventually stop!

The terms we need to check we understand here are SET and SUBSET (these are the already agreed terms used in the definition). If you didn't

understand one of these then you wouldn't have got this far yet (at least that's the idea), so let's assume we are happy with the meaning of these two.

Thus given a set S we know what is a subset of S. A subset of S is a set, of course, and sets are perfectly good (possibly abstract) objects. Consider a collection of such objects, i.e. objects each of which is a subset of S. This is itself a perfectly good set — a set of subsets of S. Now the power set of S is just the set of *all* subsets. To put it another way, it is the set with the property that if T is a subset of S, then T is an *element* of the power set of S. (The expression $\mathcal{P}(S)$ is just a *notation* for the power set.)

In SET THEORY it is useful to have a notion of 'all possible objects' which might be collected together to form sets. Unfortunately this notion is really too vague as it stands. In practice we define a UNIVERSAL set U to be a set containing all possible objects *under discussion* (with the kind of object under discussion being determined, perhaps implicitly, by the context). We usually specify a universal set *for a given problem* as some set which, at least, contains as subsets all the sets in which we are currently interested.

The COMPLEMENT of a set S (with respect to some such universal set U) is written S', and means the set of all objects in U NOT in S.

2.2.1 Cartesian product

Definition 2.6.[CARTESIAN PRODUCT] The Cartesian product of two nonempty sets S and T, written $S \times T$, is the set $S \times T$ given by

$$S \times T = \{(a, b) | a \in S \text{ and } b \in T\}$$

where $(a, b) \in S \times T$ is a constructed object made from the ordered pairing of a and b.

For example,

$$\{1, 2, 3\} \times \{x, y\} = \{(1, x), (1, y), (2, x), (2, y), (3, x), (3, y)\}.$$

Note that the order in which we write the pair $(1, x)$ (say) is important. This pair is a single element of the Cartesian product. The pair $(x, 1)$ is NOT an

element of the Cartesian product in our example (but it would be an element of $\{x, y\} \times \{1, 2, 3\}$, so obviously $S \times T \neq T \times S$ in general!).

Example 9 *Let $H = \{A, 2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K\}$ — the set of values on the cards in a 52 card deck of playing cards. Then the set $\mathcal{S}$ from example 5 may be written*

$$\mathcal{S} = H \times \{\clubsuit, \heartsuit, \spadesuit, \diamondsuit\}$$

where $(2, \clubsuit)$ represents the two of clubs, and so on. In this notation we might write $\mathcal{S}_\clubsuit = H \times \{\clubsuit\}$ (it might be safer to write $\cong$ instead of $=$, see later). We may similarly introduce $\mathcal{S}_\heartsuit = H \times \{\heartsuit\}$, and so on. Note that $\mathcal{S}_\heartsuit \cap \mathcal{S}_\clubsuit = \emptyset$; and $\mathcal{S}_\heartsuit \cup \mathcal{S}_\clubsuit \cup \mathcal{S}_\spadesuit \cup \mathcal{S}_\diamondsuit = \mathcal{S}$.

2.2.2 Aside on the subsets of the set of real numbers

We will discuss the topic of real numbers later, but in order to introduce some notation we here note that the set of real numbers, denoted $\mathbb{R}$, has a sequence of subsets:

$$\emptyset \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Exercise 4 *Explain informally the meaning of each of these symbols.*

We will also discuss $\mathbb{N}$ again later. But for now here is a 'recipe':

The set of NATURAL NUMBERS, denoted $\mathbb{N}$, satisfies *Peano's axioms*:
(a) $1 \in \mathbb{N}$;
(b) for each $n \in \mathbb{N}$ there exists a unique $n' \in \mathbb{N}$ called 'the successor of n', written $(n + 1)$;
(c) 1 is not the successor of any $n \in \mathbb{N}$;
(d) if $n' = m'$ then $n = m$;
(e) if $S \subseteq \mathbb{N}$ and $1 \in S$ and if $n \in S$ implies $(n + 1) \in S$, then $S = \mathbb{N}$.

Let us see what we get using these axioms:

$$\mathbb{N} = \{1, (1 + 1), ((1 + 1) + 1), (((1 + 1) + 1) + 1), ((((1 + 1) + 1) + 1) + 1), ...\}.$$

Of course we have a shorthand for this:

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

Exercise 5 *Give an example of a set $\overline{\mathbb{N}}$ which satisfies all of Peano's axioms except axiom (c): 1 is not the successor of any $n \in \overline{\mathbb{N}}$.*

Solution 5.1 *Without this axiom we could allow, for example,*

$$(((((1+1)+1)+1)+1)+1) = 1.$$

Then

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

(and + doesn't have its usual meaning!).

We have lots more to say about sets and numbers. We will come back to them later.

2.3 Relations and Functions

Definition 2.7. Let S and T be nonempty sets. A RELATION from S to T is any subset of $S \times T$.

For example, if S is the set of Mathematicians, and T is the set of Statisticians, then we might define a relation ρ by writing

$$\rho = \{(a, b) \in S \times T | a \text{ is older than } b\}.$$

It is often convenient to write $a\rho b$ (and say 'a has the relation ρ with b', or 'a stands in relation ρ to b', or in this case simply 'a is older than b') in case $(a, b) \in \rho$.

Note in particular than in this example (and in general) $a\rho b$ does not imply $b\rho a$!

Suppose we have a relation $\rho \subseteq S \times T$. Then

Definition 2.8.[DOMAIN] The domain of ρ, written *dom* ρ, is the set of elements of S which appear as the left hand sides of pairs which are elements of ρ.

For example, if $\rho = \{(1, x), (2, x)\}$ then $dom\ \rho = \{1, 2\}$.

Definition 2.9.[RANGE] The range of ρ, written $ran\ \rho$, is the set of elements of T which appear as the right hand sides of pairs which are elements of ρ.

In our example, $ran\ \rho = \{x\}$.

Definition 2.10.[INVERSE] The inverse of ρ, written ρ^{-1}, is the set obtained by reversing the order of each pair in ρ.

In our example $\rho^{-1} = \{(x, 1), (x, 2)\}$.

Let ρ be a relation from S to T. Then it also gives a relation from $dom\ \rho$ to T.

Exercise 6 *Show that ρ above also gives a relation from S to $ran\ \rho$.*

Solution 6.1 *This is an example of a simple kind of 'proof' of a claim, where we simply have to insert the definitions of the terms and rearrange a little:*

We have to show that $(a, b) \in \rho$ implies $b \in ran\ \rho$. But the definition of $ran\ \rho$ says that it is the set of all *right hand sides of such pairs, so certainly it includes this one!*

Exercise 7 (compulsory) *By similar means:*

1) Show that a relation ρ is also a relation from $dom\ \rho$ to any Q such that $Q \supset ran\ \rho$.

2) Show that a relation ρ is NOT a relation from $dom\ \rho$ to any P such that $P \subset ran\ \rho$.

2.3.1 Functions

Definition 2.11.[FUNCTION] A function is a relation in which each element of the domain appears exactly once as the left hand side of a pair.
In particular a relation $\rho \subseteq A \times B$ that is a function is said to be a function from A to B.
For a relation $\rho \subseteq A \times B$ that is a function, the domain A and 'codomain'

B may be indicated by writing $\rho : A \to B$.
(The modification of notation will be enlarged upon as soon as we have some examples.)

Thus the relation $\{(1, x), (2, x)\}$ is a function, but $\{(x, 1), (x, 2)\}$ is not.
To generate some more examples let us consider $A = \{a, b, c, d\}$, $B = \{r, s, t, u, v\}$. Then:
(i) $\{(a, t), (c, r), (d, s), (c, v)\}$ is not a function from A to B because c appears twice as a left-hand side of a pair; it is also not a function from A to B because b does not appear as a left-hand side;
(ii) $\{(a, u), (b, r), (c, s), (d, u)\}$ is a function;
(iii) $\{(a, c), (a, u), (b, s), (c, r), (d, t)\}$ is *not* a function;
(iv) $\{(a, u), (b, u), (c, u), (d, u)\}$ is a function;
(v) $\{(a, r), (b, s), (c, t), (d, u)\}$ is a function.

Recall that we can think of the set of real numbers $\mathbb{R}$ as the set of points on the x-axis of a Cartesian x, y frame. Then the set $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ may be represented by the points on the whole plane (i.e. with "coordinates" $(x, y) \in \mathbb{R}^2$). It follows that any subset of the points of the plane is a relation! In particular any line drawn on the plane gives a relation. We are familiar with the representation of functions from $\mathbb{R}$ to $\mathbb{R}$ by this means. On the other hand, we know that only certain lines drawn on the plane correspond to a function (an arbitrary scribble, while giving a perfectly good relation, would not normally be a function). You should compare your intuitive understanding of this with the definition above!

Since each element of the domain appears exactly once in a function, we have the opportunity for a new and neater notation. The right hand side of each pair in the function is uniquely given by the left hand side. We can recognise this by writing the pair $(x, f(x)) \in f$, say. Of course we then often go on to specify the right hand side "as a function of" the left hand side explicitly, arriving at the more familiar notation for functions, for example, if the domain is a set upon which some arithmetic operations make sense

(like $\mathbb{R}$) then we can use them:

$$f(x) = 1 + x^2.$$

Altogether we give the concrete definition of a specific function as follows. First we specify the name of the function, and the domain, and the CODOMAIN (which, note, could actually be any set containing the range). For example if f is the function, A is the domain and $B \supseteq ran\ f$ we may write

$$f : A \to B$$

and say "the function f maps the set A into the set B". Then we write

$$f : x \mapsto f(x)$$

which means that the action of f on a specific element $x \in A$ is to take it to $f(x) \in B$. In practice at this point we may be able to give $f(x)$ explicitly. For example we might write, altogether,

$$f : \mathbb{R} \to \mathbb{R}$$

$$f : x \mapsto x^3 + 3x - 2.$$

There will be examples shortly. First, here are some refinements.

2.3.2 Injection and surjection

Note that if a relation is a function $f : A \to B$ then the domain is A. The range might not be B though. Recall we have a separate name for the 'target' set B in general: *codomain*.

Definition 2.12.[ONTO] A function $f : A \to B$ is called onto (or SURJECTIVE) if $ran\ f = B$.

Note that examples (ii),(iv) and (v) above are NOT onto (recall (i) and (iii) were not even functions). We can make (ii) into an onto function by changing the codomain to $\{r, s, u\}$.

Definition 2.13.[ONE-TO-ONE] A function is one-to-one (or INJECTIVE) if

$$(\ (a,b) \in f \ \text{ and } \ (a',b) \in f\ ) \ \text{ implies } \ a = a'.$$

That is, distinct elements in A have distinct "images" in B ($f(a) \in B$ is called the "image of a under f"). Note that examples (ii) and (iv) above are not one-to-one, but that example (v) is one-to-one.

A function which is not one-to-one is called MANY-TO-ONE.

Definition 2.14.[BIJECTION] A function which is both one-to-one *and* onto is called a bijection.

Exercise 8 *Give three examples of bijections.*

There are various useful pictorial representations of functions. These will be discussed in class.

Definition 2.15.[IDENTITY FUNCTION] For each set A there is a function from A to A, called the identity function, denoted 1_A, and given by

$$1_A : A \to A$$

$$1_A : a \mapsto a.$$

Two functions h and g are said to be EQUAL as functions (written $h = g$) if they have the same domain and codomain, and $h(x) = g(x)$ for all x in the domain. For example, if h, g are two functions from $\mathbb{R}$ to $\mathbb{R}$ given by $h(x) = x + x$ and $g(x) = 2x$, then $h = g$.

The *restriction* of a function f to a subset of the domain is the function on that subset obtained by applying f to it.

2.3.3 Composition of functions

Let $f : A \to B$ and $C \supseteq ran\ f$ and $g : C \to D$. Then

Definition 2.16.[COMPOSITE FUNCTION] The composite function $g \circ f$ is defined by

$$g \circ f : A \to D$$

$$g \circ f : a \mapsto g(f(a)).$$

We write $(g \circ f)(a) = g(f(a))$.

For a relation ρ we understand $\rho(a)$ to be the *set* of objects b such that $a\rho b$. For S a subset of the domain of ρ we understand $\rho(S)$ to be the union of sets $\rho(s)$ over every $s \in S$. Relations are then composable in much the same way as functions.

Although every relation has an inverse (and hence every function has an inverse *as a relation*), not every function has an inverse which is itself a function.

Exercise 9 *Show that the inverse of a function is a function if and only if the function is a bijection.*

Exercise 10 *For $f : A \to B$ a bijection, show that*

$$f \circ f^{-1} = 1_B$$

and

$$f^{-1} \circ f = 1_A.$$

2.4 Orderings

Let P be a non-empty set.

Definition 2.17.[Partial Order Relation] A partial order relation on P, usually written $\leq$, is a relation on P to P with the following properties:

(i) $x \leq x$ for all $x \in P$ (reflexivity);

(ii) $x \leq y$ and $y \leq x$ implies $x = y$ ('anti-symmetry');

(iii) $x \leq y$ and $y \leq z$ implies $x \leq z$ (transitivity).

Then the pair $(P, \leq)$ is called a partially ordered set, or just a poset for short.

Example: For X any set then $(\mathcal{P}(X), \subseteq)$ is a poset.

Let us check this:

Reflexivity: $A \subseteq A$ for any set A, so OK.
Anti-symmetry: $A \subseteq B, B \subseteq A$ implies $A = B$, again for any two sets.
Transitivity: $A \subseteq B, B \subseteq C$ implies $A \subseteq C$, so OK.

Examples (looking ahead for a moment — using some properties of number systems):

(1) $(\mathbb{N}, \leq)$ where $\leq$ means 'less than or equal to' is a poset.

(2) $(\mathbb{N}, <)$ is NOT a poset (it fails reflexivity test).

(3) $(\mathbb{Z}, a$ divides $b)$ is NOT a poset (1 divides -1, and -1 divides 1).

(4) $(\mathbb{N}, a$ divides $b)$ is a poset.

(5) For X a nonempty set, the set of all real valued functions $f : X \to \mathbb{R}$, with relation $f \leq g$ iff $f(x) \leq g(x)$ for all $x \in X$, is a poset.

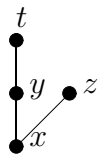
2.4.1 Diagrammatic representation of posets: Hasse diagrams

In a Hasse diagram we take informal advantage of the similarity of the definition to the 'height ordering' of the vertical line to represent certain posets as follows. We draw a 'node' or spot for each element of the set, and a bond between distinct nodes x and y (say) if either $x \leq y$ or $y \leq x$ (if there is some z such that $x \leq z \leq y$ we only draw bonds between x and z and between z and y, since this automatically creates a connection path for us between x and y). We draw y ABOVE x on the page if $x \leq y$.

For example: (1) Consider the set $S = \{x, y\}$ with partial order given by $x \leq y$ (here note that $x \leq x$ and $y \leq y$ may be understood implicitly). Then the diagram is

If you like, you can even put an arrow on the edge from y to x (thus a 'down' arrow). To be clear, in general t (say) just being above x on the page is not enough to indicate a relation $x \leq t$, but first there must also be an edge drawn.

(2) $S = \{x, y, z, t\}$ with $x \leq y, y \leq t, x \leq z$ (and $x \leq x, y \leq y, z \leq z, t \leq t$ and $x \leq t$ implicitly) is



We will give some more examples in the lecture.

2.4.2 Structure of ordered sets

Definition 2.18.[Comparability] In a poset $(P, \leq)$ two elements $x, y \in P$ are said to be comparable iff $x \leq y$ or $y \leq x$ (i.e. if joined by a descending line in the Hasse diagram, if there is one).

For example, in $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$ the elements $\{1\}$ and $\{2\}$ are NOT comparable, but $\{1\}$ and $\{1, 2\}$ are comparable.
Then again in $(\mathbb{N}, m$ divides $n)$ we have that 4 and 6 are not comparable but 3 and 6 are comparable.

Definition 2.19.[Total Ordering] A poset in which every pair of elements is comparable is called a total ordering, or a linear ordering, or a CHAIN.

For example $(\mathbb{N}, \leq)$ is a chain; $(\mathcal{P}(X), \subseteq)$ is not a chain; and $(\mathbb{N}, a$ divides $b)$ is not a chain.

Definition 2.20. A linear ordering $\leq$ on a set P in which every non-empty subset has a LEAST ELEMENT (i.e. an element l such that $l \leq x$ for all x in the subset) makes $(P, \leq)$ a WELL ORDERED SET.

We are not quite ready to give good examples for well-ordered sets. But if we appeal to a little bit of 'knowledge' from elsewhere for a moment, then we can think about some meta-examples...

Proposition 2.21.*[Exercise: think about these claims.]*

1. *With its 'usual' meaning, we have that* $(\mathbb{N}, \leq)$ *is well ordered.*
2. *Every finite chain is well ordered.*

3. $(\{x \in \mathbb{Q} \,:\, x \geq 0\}, \leq)$ *is NOT well ordered.*

2.4.3 Ordinals

If $(P, \leq)$ is a totally ordered set (and we write $p < q$ to mean $p \leq q$ and $p \neq q$), then we may use the following definition:

$$P_{<a} \;:=\; \{x \in P \mid x < a\}$$

An *ordinal* is a well-ordered set $(P, \leq)$ such that $P_{<a} = a$ for all $a \in P$.

This definition looks a bit strange, but the best way to address that is to work with it.

Firstly observe that there is at least one ordinal, since $\emptyset$ satisfies the conditions trivially — or rather vacuously. Next suppose $(P, \leq)$ is a non-empty ordinal. Then (by the well-ordered property) it has a least element, ω say. Since ω is least we have $P_{<\omega} = \emptyset$. By the definition of ordinal we have $P_{<\omega} = \omega$ so $\omega = \emptyset$. That is, the least element of any non-empty ordinal is $\emptyset$. A single element set is a well-ordered set (by taking the reflexive relation), and $P = \{\emptyset\}$ has the property $P_{<\emptyset} = \emptyset$ so this P is ordinal.

Now supppose P is not simply $\{\emptyset\}$, i.e. it contains at least one more element. Call the least element in $P \setminus \{\emptyset\}$ by p. Then $p = P_{<p} = \{\emptyset\}$. Thus every ordinal that is not $\emptyset$ or $\{\emptyset\}$ contains both. Indeed we see that $\{\emptyset, \{\emptyset\}\}$ is ordinal, with $\emptyset < \{\emptyset\}$.

If an ordinal P is not any of the three so far then it contains $\emptyset$ and $\{\emptyset\}$ and at least one more element. Again call the least element in the complement by p. Then $p = P_{<p} = \{\emptyset, \{\emptyset\}\}$. Indeed we see that $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ is ordinal, with $\emptyset < \{\emptyset\} < \{\emptyset, \{\emptyset\}\}$.

Observe now that we can iterate this process, at each stage adding one more (ugly but well-defined and distinct) new element:
If P is an ordinal then $P \cup \{P\}$ is an ordinal, with $p < P$ for all $p \in P$.
The construction does not terminate.

The ordinals we have constructed look a bit ugly Everyone's favourite

notation for them is to use the symbols 0 for $\emptyset$; 1 for $\{\emptyset\}$; 2 for $\{\emptyset, \{\emptyset\}\}$; 3 for $\{0, 1, 2\}$; and so on. In other words, every natural number is associated to an ordinal, and the order on the ordinals gives everyone's favourite order on the natural numbers.

The ordinals go beyond the natural numbers. We can consider a smallest ordinal (call it w, say) that is not a natural number — then w is the set of all natural numbers, and the next ordinal after w is $w \cup \{w\}$. And so we can go on! We will come back to this journey later.

2.4.4 More on posets

Definition 2.22.[BOUNDEDNESS] A poset $(P, \leq)$ in which there exists an element, $\perp$ (say), such that $\perp \leq x$ for all $x \in P$, and an element, $\top$ (say), such that $x \leq \top$ for all $x \in P$ is said to be BOUNDED.
For example:

1. $(\mathcal{P}(S), \subseteq)$ is bounded (even when S is infinite). Exercise: What are $\perp$ and $\top$ here?

2. $(\{1, 2, 3, 4, 6, 9\}, a \text{ divides } b)$ has no $\top$, so is not bounded (exercise: draw the diagram).

Definition 2.23.[MAXIMAL/MINIMAL ELEMENTS] In a poset $(P, \leq)$ an element $x \in P$ is MAXIMAL iff $y \geq x$ implies $y = x$ (i.e. x is not $\leq$ any *other* element).

Similarly for MINIMAL elements.

e.g.1. in $(\{1, 2, 3, 4, 6, 9\}, a \text{ divides } b)$ the elements 4,6,9 are maximal.
e.g.2. in a bounded poset $\top$ (also called 'the top element') is the unique maximal element, and $\perp$ (also called 'the bottom element') is uniquely minimal.

Definition 2.24.[LOWER BOUND] In $(P, \leq)$ let A be a nonempty subset of P. Then $x \in P$ is a LOWER BOUND of A if $x \leq a$ for all $a \in A$.

Definition 2.25.[GREATEST LOWER BOUND / INFIMUM] With A as above, x is a GLB (or 'inf') of A if $x \geq$ every lower bound of A.

Exercise 11 *If $inf\ A$ exists it is unique. Prove it!*

Similarly, y is an UPPER BOUND of A if $y \geq a$ for all $a \in A$, and y is a LEAST UPPER BOUND (or SUPREMUM, or 'sup') if it is $\leq$ every upper bound of A.

Example: $(\mathbb{N}, \text{is a factor of})$ - let $A = \{4, 6\}$, then 12,24,36,... are all upper bounds for A; 1,2 are lower bounds.

Sup $A = 12$ (Lowest Common Multiple (LCM) of 4 and 6)

Inf $A = 2$ (Highest Common Factor (HCF) of 4 and 6).

Proposition 2.26.*[Zorn's Lemma (see later)] A poset P in which every chain has an upper bound has a maximal element.*

There are some more advanced notes on posets (specifically on LATTICES) to be found in the version of these notes published on the maths web pages. Of course, looking at these additional notes is optional.

2.5 Equivalence Relations

Let ρ be a relation from set A to A (i.e. $\rho \subseteq A \times A$). Then

Definition 2.27.[REFLEXIVE/SYMMETRIC/TRANSITIVE] .

1. ρ is reflexive if and only if $a\rho a$ for all $a \in A$.
2. ρ is symmetric if and only if whenever $a\rho b$ then $b\rho a$.
3. ρ is transitive if and only if whenever ($a\rho b$ and $b\rho c$) then $a\rho c$.

Examples:

$\rho =$ "belongs to the same family as" is reflexive, symmetric and transitive;

$\rho =$ "is an ancestor of" is transitive;

$\rho =$ "is the mother of" is none of these!

Definition 2.28.[EQUIVALENCE RELATION] A reflexive, symmetric, transitive relation is an equivalence relation.

Such a relation is often written $\sim$ (as in $a \sim b$) unless it already has a name.

For specific relations, we usually define a pair, consising of the set A together with its equivalence relation: $(A, \sim)$. Thus we have:

(1) $(\mathbb{N}, =)$ given by $a\rho b$ if and only if $a = b$;

(2) $(\mathbb{Z}, \sim)$ given by $a \sim b$ if and only if $5|(a-b)$ (here we have introduced the following

Definition 2.29.[DIVIDES] For $n, m \in \mathbb{Z}$ we say p divides m, and write $p|m$ (*not* to be confused with p/m), in case the equation $m = pn$ is solved by some $n \in \mathbb{Z}$.

for example here $11 \sim 1$ (i.e. $5|(11-1)$) since $11 - 1 = 5.2$ - see later). Let's check these:

In (1) we have $a = a$ for any number a, so the relation is reflexive; if $a = b$ then certainly $b = a$, so it is symmetric; and if $a = b$ and $b = c$ then $a = c$, so transitive;

(2) is more of a challenge, we have $(a - a) = 0$ and $5|0$, so reflexive; we have $(a-b) = -(b-a)$, so if $5|(a-b)$ then $5|(b-a)$, so symmetric; and finally if $(a - b) = 5k$ (say) and $(b - c) = 5l$ (with $k, l \in \mathbb{Z}$) then $(a - c) = 5(k - l)$, so transitive!
The relation (2) is sometimes written $a \equiv b$ (mod.5).

2.5.1 Equivalence classes

Definition 2.30.[EQUIVALENCE CLASS] Given a pair $(A, \sim)$ we define the equivalence class containing $a \in A$ to be the set

$$[a] = \{x \in A \ : \ x \sim a\}.$$

Note that $[a] \subseteq A$; $a \in [a]$; and if $b, c \in [a]$ then $a \sim b, c \sim a$ and indeed $b \sim c$ (i.e. *any* two elements of the same class are equivalent).

Theorem 1 (On equivalence classes) *Let $\sim$ be an equivalence relation on a set A and let $[a]$ be the equivalence class of $a \in A$. Then for any $a, b \in A$*

(i) $[a] = [b]$ *if and only if* $a \sim b$*;*
(ii) if $[a] \neq [b]$ *then* $[a] \cap [b] = \emptyset$*.*

Proof: The theorem may be broken into three parts. Firstly, the 'if' part of (i):

We can write this part $[a] = [b] \Leftarrow a \sim b$, so this is what we need to show. In other words we must show that if we *assume* $a \sim b$, then $[a] = [b]$ follows, so.... Let $a \sim b$. Then by definition $a \in [b]$. Then again, $[a] \subseteq [b]$, since if $x \in [a]$ then $x \sim a$, but $a \sim b$ and so by transitivity $x \sim b$, that is $x \in [b]$. Similarly $[b] \subseteq [a]$, so finally $[a] = [b]$.
Now the 'only if' part of (i) (i.e. to show $[a] = [b] \Rightarrow a \sim b$):

If $[a] = [b]$ then since $b \sim b$ we have $b \in [a]$ and so $b \sim a$;
Lastly, part (ii):

We will prove this by CONTRADICTION. This means we assume the *opposite* to what is required, and prove this must be false (if the opposite is false, then logically the statement itself must be true). The trick here is to figure out what the opposite of the statement is! This is not always obvious, but in our case the opposite would be:

a and b can be found such that $[a] \neq [b]$ but $[a] \cap [b] \neq \emptyset$.

Let's assume *this* statement true, and see what happens. Consider such an a and b, and consider any $x \in [a] \cap [b]$. If it exists (the last ingredient of the statement says it does!) then this means $x \sim a$ and $x \sim b$. This then implies $a \sim b$ by symmetry and transitivity. But part (i), which is already proved, says that *this* can only happen when $[a] = [b]$ — a contradiction between the consequences of the first and second ingredients of the statement. The only resolution is that there can be no such x — that is, $[a] \cap [b] = \emptyset$. QED.

There will be more examples of this kind of proof shortly.

Definition 2.31.[PARTITION] Given a set A, if there exists a set I and a collection of nonempty subsets $\{X_i \mid i \in I\}$ of A such that

(i) $x \in A$ implies $x \in X_i$ for some $i \in I$;

(ii) $X_i \cap X_j = \emptyset$ unless $i = j$,

then the collection $\{X_i \mid i \in I\}$ is said to form a partition of A.

So BY THEOREM 1 an equivalence relation $\sim$ on a set A defines a partition of A into its equivalence classes.
Example: $(\mathbb{Z}, \sim)$ where $a \sim b$ iff $(a - b)$ divisible by 5.

We have

$$[0] = \{...., -10, -5, 0, 5, 10, 15, ...\}$$

$$[1] = \{...., -9, -4, 1, 6, 11, 16, ...\}$$

$$[2] = \{...., -8, -3, 2, 7, 12, 17, ...\}$$

and $[3], [4]$ similarly (exercise). Altogether there are five classes partitioning the integers $\mathbb{Z}$. Sometimes we write these classes simply as $0, 1, 2, 3, 4$ 'modulo 5' (or mod 5). Note that $[0] = [5] = [10] = ...$, and $[3] = [8] = [13] = ...$ and so on.

The SET OF EQUIVALENCE CLASSES here has five elements and is written $\mathbb{Z}_5$ - sometimes called the set of 'residues' mod 5. We can do 'mod 5' arithmetic, as in

$$4 + 3 = 2 \qquad\qquad mod\ 5.$$

This can be done for residue classes modulo any integer. For example we have a complete arithmetic 'mod 3':

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

.

Conversely, given a partition of A we can define an equivalence relation on A by $a \sim b$ iff a, b belong to the same set X_i of the partition. For example: Let $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 0\}$ with partition $\{1, 2, 0\}, \{3\}, \{4, 5, 7\}, \{6, 8\}, \{9\}$; then the corresponding equivalence relation is

$$\{(1,1), (2,2), (3,3), (4,4), (5,5), (6,6), (7,7), (8,8), (9,9), (0,0), (1,2), (2,1), (1,0),$$

$$(0,1), (2,0), (0,2), (6,8), (8,6), (4,5), (5,4), (4,7), (7,4), (5,7), (7,5)\}.$$

2.6 Countability

Consider the collection $\mathfrak{A}$ of all sets (this is a potentially dangerous notion — see [Cohn] on *Russell's Paradox* — but the dangers need not concern us here). We can define a relation $\sim$ on this collection as follows. For $X, Y \in \mathfrak{A}$ let $X \sim Y$ iff there exists a bijection $f : X \to Y$. Note

(i) $1_X : X \to X$, so $\sim$ is reflexive;

(ii) If $f : X \to Y$ is a bijection, then $f^{-1} : Y \to X$ is a bijection, so $\sim$ is symmetric;

(iii) $f : X \to Y$ and $g : Y \to Z$ bijections implies $(g \circ f) : X \to Z$ is a bijection, so $\sim$ is transitive.

Altogether then, we have an equivalence relation.

In some sense (and precisely for the finite sets) each equivalence class contains all the sets with the same 'number of elements'.

For a set A the equivalence class $[A]$ under the relation $\sim$ is written $Card\ A$ ('Cardinal A'). We have that $Card\ A = Card\ B$ iff A, B are 'numerically equivalent'.

For *finite* sets the equivalence class of all sets containing n elements is sometimes written simply as n. This n is called a 'cardinal number' (in general such numbers are the numbers associated with set sizes - but the finite cardinal numbers are the natural numbers $n \in \mathbb{N}$).

A set in $Card\ \mathbb{N}$ is called COUNTABLY INFINITE. A *countable set* is either finite or infinite. A set is countable, it 'can be counted', if when one sets out to count the elements (i.e. assign a distinct number to each of them from 1,2,3,...) there is a way of doing this such that any given element of the set eventually gets counted. N.B. This is not the same as saying that *all* the elements will be counted in finite time. $Card\ \mathbb{N}$ is sometimes denoted $\aleph_0$ ('aleph zero').

Example:

$$E = \{2, 4, 6, 8, 10, 12, ...\} \subset \mathbb{N}$$

what is the cardinality of E? Well,

$$f : \mathbb{N} \to E$$

$$f : x \mapsto 2x$$

is a bijection (check it!), so $Card\ E = \aleph_0$.

Obviously $\aleph_0$ is not any finite cardinal number. In a sense it is *bigger*. In a similar sense, as we will see shortly, there are still bigger infinite numbers (i.e. there are infinite sets too big to have a bijection with $\mathbb{N}$)! We call $\aleph_0$ a TRANSFINITE NUMBER. We have the following transfinite arithmetic:

$$2\,\aleph_0 \;=\; \aleph_0$$

(since naively we threw away half the elements of $\mathbb{N}$ to get E, and yet it didn't change the cardinality)

$$\aleph_0 + \aleph_0 = \aleph_0$$

$$\aleph_0 + 1 = \aleph_0$$

....so, is every infinite set countable? Well, what sets do we know which are bigger than $\mathbb{N}$? Obviously we have the rational numbers - even the set $\mathbb{Q}_+$ of positive rational numbers obeys $\mathbb{Q}_+ \supset \mathbb{N}$, but in fact:

Proposition 2.32. $Card\ \mathbb{Q}_+ = \aleph_0$

Proof: We will list the elements of $\mathbb{Q}_+$ in such a way that a bijection with $\mathbb{N}$ (i.e. a way of 'counting' the elements such that any given element is eventually counted) can be explicitly given.

We organise the elements of $\mathbb{Q}_+$ as follows:

$$1/1 \quad 1/2 \quad 1/3 \quad 1/4 \quad 1/5 \quad ...$$

$$2/1 \quad 2/2 \quad 2/3 \quad 2/4 \quad 2/5 \quad ...$$

$$3/1 \quad 3/2 \quad 3/3 \quad 3/4 \quad 3/5 \quad ...$$

$$...$$

(here many elements are counted more than once, but at least we can be sure that eventually any given element does appear on the grid). Now suppose we consider an arbitrary element, which is of the form $x = p/q$ by definition. Each South-East diagonal of the grid gives all the numbers with fixed $p + q$. We will count through the grid starting from the top left and then counting up each such diagonal in turn (i.e. running through the diagonals in order $p + q = 2, 3, 4, 5, ...$). That is, our bijection will be:

$$f(1/1) = 1$$

$$f(2/1) = 2$$

$$f(1/2) = 3$$

$$f(3/1) = 4$$

(2/2 has already been counted as 1/1)

$$f(1/3) = 5$$

$$f(4/1) = 6$$

and so on. QED.
You should check that you *understand* how the one-to-one and onto conditions are satisfied here.

Corollary 1 (Exercise) $Card\, \mathbb{Q} = \aleph_0$.

So we still havn't found any bigger 'numbers' than $\aleph_0$, even though $\mathbb{Q}$ contains $\mathbb{N}$ and much much more. What about the even bigger set $\mathbb{R}$?

Proposition 2.33. $Card\, \mathbb{R} \neq \aleph_0$.

Proof: We will prove the proposition by contradiction! In other words we will assume that $\mathbb{R}$ is countable, and prove that this must be wrong.

If we assume that $\mathbb{R}$ is countable then any subset must also be countable (if every element can be counted, then every element of a subset can be counted). Let us consider the set $(0, 1) \subset \mathbb{R}$, which is the set of real numbers

between 0 and 1. Our assumption implies that $(0,1)$ is countable, so that each $x \in (0,1)$ may be numbered distinctly by some function f, a bijection onto the natural numbers. Since it is a bijection it has an inverse f^{-1}, i.e. for each natural number n there is a unique real number $f^{-1}(n)$ in the interval $(0,1)$.

Now consider an $x \in (0,1)$ written in decimal form. This form may be familiar to you. For example $x = .7 = .70000...$ (recurring 0s) or $x = .76582342222....$ (recurring 2s), or $x = \pi - 3 = .1415926...$ (no recuring pattern!). Note that to avoid duplicating values x we can avoid recurring 9s. To see why recurring nines are redundant consider, say, .79999... (recurring 9s) and .80000... (recurring 0s). The calculation $9 \times .79999... = (10 \times .79999...) - .79999... = 7.9999... - .79999... = 7.2$ shows that $.79999... = .8$. Now consider a particular decimal

$$y = .a_1a_2a_3a_4....$$

(e.g. $y = .2343479....$, so each $a_i \in \{0,1,2,3,4,5,6,7,8,9\}$). Suppose that for all i, the i^{th} decimal place - a_i - is chosen to be *different from* the i^{th} decimal place of the real number $f^{-1}(i)$. For example a_1 is different from the first decimal place of $f^{-1}(1)$; a_2 is different from the first decimal place of $f^{-1}(2)$; and so on.

By this construction y differs from each and every element of the list of images of f^{-1} in at least one decimal place. But of course if two numbers are the same then (excluding the situation with recurring 9) they must be the same in every decimal place, so y is actually a different number from each and every element of the list. But it is of the form $y = .a_1a_2....$, so certainly $y \in (0,1)$. But then f^{-1} is not onto, so it is not a bijection, so neither is f, which is then a CONTRADICTION of the original assumption.

We conclude that the assumption must be wrong, that is $(0,1)$ is 'uncountable'. Then $\mathbb{R}$ is uncountable. QED.

Now we can introduce a new 'number': $Card\ \mathbb{R}$, which is often written C for 'continuum'.

This raises some intriguing questions. For example: Are there any cardinal numbers 'between' $\aleph_0$ and C? Are there numbers bigger than C? The mathematician CANTOR has thought a lot about these problems, with limited success. For the first question we have 'Cantor's continuum hypothesis', in which he claims that there are no cardinal numbers between $\aleph_0$ and C. What do you think?.....

For the second question - let us recall the notion of power set $\mathcal{P}(S)$ - the set of all subsets of S.

Exercise 12 *Verify that for finite sets*

$$|\mathcal{P}(S)| = 2^{|S|}.$$

In general considering $Card\ \mathcal{P}(S)$ (which we may abuse notation to write as $2^{Card\ S}$) is a reasonable way of trying to generate new cardinals. Cantor proved that $Card\ \mathcal{P}(S) > Card\ S$ continues to hold for transfinite numbers, so there exist infinitely many transfinite cardinals:

$$\aleph_0, 2^{\aleph_0}, 2^{2^{\aleph_0}}, ...$$

Exercise 13 (Difficult) *Prove that* $Card\ \mathcal{P}(\mathbb{N}) = 2^{\aleph_0} = C$.

Definition 2.34.[$\aleph_1$] We define $\aleph_1$ to be the next bigger cardinal after $\aleph_0$. This raises the question: Is $\aleph_1 = C$? What do you think?...

2.7 Permutations

If the number of elements in a set is a natural number (i.e. if it is finite, since then it is certainly a non-negative whole number!) then the set is called a finite set. For example, $A = \{a, b, c, d, e, f, g\}$ is a finite set, as it has 7 elements; meanwhile $\mathbb{R}$ is not a finite set. We will return to this point later.

Definition 2.35.[ORDER] The order (or degree) of a finite set A, denoted $|A|$, is the number of elements in the set.

Denoting the set of all finite sets by F, then the 'order' operation is a function

$$\text{Order} : F \to \mathbb{N}$$

i.e.

$$\text{Order} : A \mapsto |A|.$$

For example, if $B = \{a, b, c, d\}$ then $\text{Order}(B) = |B| = 4$.

Definition 2.36.[PERMUTATION] A bijection $f : A \to A$ on a finite set A is called a permutation of A.

For example, if $S = \{1, 2, 3, 4\}$ then f given by $f(1) = 2$, $f(2) = 3$, $f(3) = 4$, $f(4) = 1$ is a permutation. Permutations may be written in the form

$$\begin{pmatrix} a & b & c & ... & x \\ f(a) & f(b) & f(c) & ... & f(x) \end{pmatrix}.$$

This one then becomes

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

Exercise 14 *Verify that any $f : A \to A$ is 1–to–1 if and only if it is onto.*

Let A be a finite set of degree n, and f be a permutation of A. If repeated composition of f with itself produces the identity function after $|A|$ compositions and not before (or, equivalently, if for any $x \in A$ we have that $\{x, f(x), (f \circ f)(x), (f \circ (f \circ f))(x), ...\} = A$) then the permutation is called a CYCLE of A, or n–CYCLE. More generally, if f restricts to a cycle of B for some $B \subset A$, and acts as $f(x) = x$ for all $x \notin B$, then f is a $|B|$–cycle. (Note that there are no permutations of A which are p-cycles with $p > n$.)

Exercise 15 *Show that the f defined in the example above is a cycle. Give an example of a bijection $g : S \to S$ which is not a cycle.*

Exercise 16 *Let A be the set of letters in the alphabet, together with the hyphen symbol – (so $|A| = 27$). Let A' be the subset of these symbols occuring at least once in the word* gerbil–brain. *Write down A'.*

Let $f : A' \to \mathbb{N}$ be the alphabetical ordering of these symbols (so $f(a) = 1$, $f(b) = 2$, $f(e) = 3$, and so on) with $f(\text{–}) = 9$. Note that $|ran\ f| = 9$. Determine the word obtained by applying the inverse of f to the sequence of elements of $ran\ f$ given by 1653791643281.

Chapter 3

Complex Numbers

The set $\mathbb{N}$ of natural numbers is closed under the operation of addition, but not under the operation of subtraction.
The set $\mathbb{Z}$ of integers is closed under the operation of addition, and under the operation of subtraction, *and* under the operation of multiplication, but not under the operation of division.
The set $\mathbb{Q}$ of rational numbers is closed under $+, -, \times$ and divide. Thus we can solve any equation of the form

$$ax + b = 0$$

where a, b are rational ($a \neq 0$) with rational x.

However, we cannot solve

$$x^2 - 2 = 0$$

with rational x. We need $\sqrt{2}$, and this is not rational. Suppose we add $\sqrt{2}$ to the set of numbers $\mathbb{Q}$. More generally, suppose we consider the extension of the set $\mathbb{Q}$ to the set $\mathbb{Q}[\sqrt{2}]$ of all numbers of the form

$$a + \sqrt{2}b$$

where $a, b \in \mathbb{Q}$. This set is closed under +,-, x and divide.

Exercise 17 *Show that* $\mathbb{Q}[\sqrt{2}]$ *is closed under all the arithmetic operations.*

With $\mathbb{Q}[\sqrt{2}]$ we can solve the quadratic equation above — but not *all* quadratics. Adding all the numbers needed to solve such equations into our set, we get more and more of the set $\mathbb{R}$ of real numbers. (In fact we do not get *all* real numbers in this way, but let us leave the story of π and e and the *transcendental* numbers for later!). However, even if we do consider *all* the real numbers we cannot find a solution to

$$x^2 + 1 = 0$$

So consider adding $\sqrt{-1}$ to $\mathbb{R}$. In this way we get the set of *complex numbers* $\mathbb{C}$. This is the set of all numbers of the form

$$z = a + ib$$

where a, b are real numbers and $i = +\sqrt{-1}$.

Every polynomial equation has a solution in $\mathbb{C}$. In this sense (and in a number of other ways which we will discuss shortly) complex numbers are very useful. The presence of i may seem alarming, but in fact we can do arithmetic with complex numbers rather like we can with $\mathbb{Z}[\sqrt{2}]$ or $\mathbb{Q}[\sqrt{2}]$.

Example: $(7 + 2i) + (1 - i\pi) = 8 + i(2 - \pi)$.

Exercise 18 *Try some complex arithmetic. What is* $(3 + 4i) + (1 - 2i)$*?*

What is $(3 + 4i)(1 - 2i)$*?*

What is $(3 + 4i)/(1 - 2i)$*?*

Notation:

$$Re(x + iy) = x$$

is the *real part of* $x + iy$;

$$Im(x + iy) = y$$

is the coefficient of the *imaginary part of* $x + iy$.

(Two complex numbers are *equal* only if their real parts are the same *and* their imaginary parts are the same.)

Define *magnitude*:

$$|x + iy| \ = \ +\sqrt{x^2 + y^2}$$

For example $|4+3i| = +\sqrt{16+9} = 5$.
With $z = x + iy$ define

$$z^* = x - iy$$

so that

$$|z|^2 = zz^*$$

3.1 Polar representation and Argand diagram

Since a complex number has two real coefficients it is a little like an element of $\mathbb{R}^2$. Indeed there is a bijection between the set $\mathbb{R}^2$ and the set $\mathbb{C}$ given by

$$(x, y) \mapsto x + iy$$

In this sense we can represent $z \in \mathbb{C}$ on the Cartesian plane, i.e.

$$z = x + iy$$

When we do this, we call the representation an *Argand diagram*. With this geometrical picture of complex numbers we can describe them another way: by giving the distance r from $(0, 0)$ to (x, y), together with the angle θ made by the x-axis and the line from $(0, 0)$ to (x, y).

Exercise 19 *Draw a picture of $z = 3 + 4i$ on the Cartesian plane and work out r and θ.*

The *polar coordinate* version may be written

$$z = r(\cos(\theta) + i\sin(\theta)) = re^{i\theta} \tag{3.1}$$

(here the first equality is just trigonometry, while the second is more interesting — a very useful representation, as we will see). Note that z is unchanged by adding 2π to θ. Thus while x, y can take any real value, $r \geq 0$ (it is a distance!) and $0 \leq \theta \leq 2\pi$ (it is an angle).

Exercise 20 *Draw pictures of* $z = 1, 0, -1, i, -i$*, and work out their* $re^{i\theta}$ *representations.* [1]

We have

$$(re^{i\theta})(r'e^{i\theta'}) = rr'e^{i(\theta+\theta')}$$

Exercise 21 *Prove the double angle formulas from trigonometry using this idea.*

Prove the triple angle formulas from trigonometry using this idea!! [2]

Note also that

$$|re^{i\theta}| = r$$

$$(re^{i\theta})^{-1} = r^{-1}e^{-i\theta}$$

and

$$\sqrt{re^{i\theta}} = +\sqrt{r}e^{i\theta/2}$$

For example

$$\sqrt{i} = \frac{1}{\sqrt{2}}(1+i)$$

---

[1] Some Answers:

$$1 = 1e^{i0} = 1e^{i2\pi} = \dots$$

$$0 = 0e^{i\theta}$$

where θ can be anything $0 \le \theta \le 2\pi$;

$$-1 = 1e^{i\pi} = 1e^{-i\pi} = \dots$$

$$i = 1e^{i\pi/2}$$

[2] The idea:

$$(\cos\theta + i\sin\theta)^n = (e^{i\theta})^n = e^{in\theta} = \cos n\theta + i\sin n\theta$$

so equating the real parts of the left and right hand side when $n = 2$ (say) gives

$$(\cos\theta)^2 + (i)^2(\sin\theta)^2 = (\cos\theta)^2 - (\sin\theta)^2 = (\cos\theta)^2 - (1-(\cos\theta)^2) = 2(\cos\theta)^2 - 1 = \cos 2\theta.$$

(In other words, if you remember equation (3.1) you need never forget a trig formula again!)

Exercise 22 *Check this, and draw the argand diagram.*

Indeed

$$(re^{i\theta})^{1/3} = r^{1/3}e^{i(\theta+2\pi n)/3}$$

where $n \in \mathbb{Z}$. Notice that there are three *distinct* solutions to this — the three *cube roots* of $z = re^{i\theta}$.

Exercise 23 *Plot the three cube roots of* -1 *on an Argand diagram, solutions to* $z^3 = -1$.

Now do exercise sheet 4.

Chapter 4

Sequences and Series

4.1 Summation of series

Let $a_1, a_2, a_3, \ldots$ be a sequence of numbers. Define

$$S_n = \sum_{i=1}^{n} a_n.$$

The problem is, given the sequence, to work out the sum S_n. In this chapter we will look at ways to compute this sum for a variety of types of sequence.

Almost trivial example:

$$\sum_{i=1}^{n} 1 = n.$$

4.1.1 Generalities

First, note that $\sum_{i=1}^{n} -$ is a *linear* operation. What does this mean?

For example, suppose a sequence is described by some function, i.e. $a_i = g(i)$. Let us write

$$S_n(g) \ := \ \sum_{i=1}^{n} g(i).$$

Linearity means that given two functions $g(i)$ and $h(i)$ and two constants a, b we have

$$\sum_{i=1}^{n}(ag(i) + bh(i)) = aS_n(g) + bS_n(h)$$

(just like with integration).

From our almost trivial example we have

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

4.1.2 Method of differences

Suppose there is some function $f(i)$ such that

$$a_i = f(i+1) - f(i)$$

for all i. Then

$$S_n = a_1 + a_2 + a_3 + \ldots + a_{n-1} + a_n$$

$$= f(2)-f(1)+f(3)-f(2)+f(4)-f(3)+\ldots+f(n)-f(n-1)+f(n+1)-f(n)$$

$$= f(n+1) - f(1).$$

In other words the sum reduces to computing one single difference! This is wonderful. The real problem is *finding* a suitable function $f(n)$. There is no good general method to do this. The idea does have utility though — through adapting a set of examples which do work. If you like, we turn the problem on its head: *Given* a function $f(n)$, what sequence do we get?!

Examples: Let $f(i) = i^2$. Then $a_i = (i+1)^2 - i^2 = 2i + 1$. Thus

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

but

$$\sum_{i=1}^{n}(2i+1) = 2\left(\sum_{i=1}^{n} i\right) + \left(\sum_{i=1}^{n} 1\right) = 2\left(\sum_{i=1}^{n} i\right) + n$$

so altogether

$$\left(\sum_{i=1}^{n} i\right) = \frac{n(n+1)}{2}.$$

This is a result you will already be familiar with (or easily verify by elementary means), but it serves to make the point.

Now consider $f(i) = i^3$. Then $a_i = (i+1)^3 - i^3 = 3i^2 + 3i + 1$. Thus

$$\sum_{i=1}^{n}(3i^2 + 3i + 1) = (n+1)^3 - 1 = n^3 + 3n^2 + 3n = n(n^2 + 3n + 3)$$

but

$$\sum_{i=1}^{n}(3i^2 + 3i + 1) = 3\left(\sum_{i=1}^{n} i^2\right) + 3\left(\sum_{i=1}^{n} i\right) + \left(\sum_{i=1}^{n} 1\right)$$

$$= 3\left(\sum_{i=1}^{n} i^2\right) + 3\frac{n(n+1)}{2} + n$$

so

$$\left(\sum_{i=1}^{n} i^2\right) = \frac{(n^3 + 3n^2 + 3n) - (3\frac{n(n+1)}{2} + n)}{3}$$

$$= \frac{2(n^3 + 3n^2 + 3n) - (3n(n+1) + 2n)}{6} = \frac{2n^3 + 6n^2 + 6n - 3n^2 - 3n - 2n}{6}$$

$$= \frac{2n^3 + 3n^2 + n}{6} = \frac{(2n+1)(n+1)n}{6}$$

which is less obvious!

It will be clear that we can compute $\sum_{i=1}^{n} i^r$ for any positive integer r in the same way. Note that this means that we can compute

$$\sum_{i=1}^{n} P(i)$$

where $P(i)$ is any polynomial!

Another example: we can sum $\sum_{i=1}^{n} \frac{1}{i(i+1)}$ by noting that

$$a_i = \frac{1}{i} - \frac{1}{i+1}$$

so

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \left(-\frac{1}{n+1}\right) - (-1). \tag{4.1}$$

(Again this idea can be adapted to solve a number of such problems — see the exercises.)

Another example: consider $\sum_{i=1}^{n} k^i$, where k is any number (called a *geometric series*). Note that

$$(1-k)(1+k+k^2+k^3+\ldots+k^n)$$

$$= (1+k+k^2+k^3+\ldots+k^n) - k(1+k+k^2+k^3+\ldots+k^n) = 1-k^{n+1}$$

so

$$\sum_{i=1}^{n} k^i = \frac{1-k^{n+1}}{1-k} \tag{4.2}$$

4.2 Infinite Series

It is possible (depending on the sequence) that

$$S = \lim_{n\to\infty} S_n$$

is well defined (i.e. there is a finite limit value). [1] In this case the infinite series is said to be *convergent*. (Otherwise it is *divergent*.)

Example: $\sum_{i=1}^{\infty} \frac{1}{2^i} = 1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \ldots = 2$, but $\sum_{i=1}^{\infty} 1$ is divergent.

The series from equation(4.1) is convergent, since

$$S = \lim_{n\to\infty} \left(1 - \frac{1}{n+1}\right) = 1$$

[1] Recall that if we can make $f(x)$ take values arbitrarily close to some number l by choosing x close enough to some number p then we say l is the *limit* of $f(x)$ at p.

For example $\lim_{n\to\infty} \frac{1}{n} = 0$, since we can make $\frac{1}{n}$ arbitrarily small by making n large enough. Similarly $\lim_{n\to\infty} \frac{1}{n^r} = 0$ for any positive number r.

Another more subtle example: $\lim_{\theta\to 0} \frac{\sin\theta}{\theta} = 1$.

The series from equation(4.2) is convergent provided $|k| < 1$, since

$$S = \lim_{n\to\infty} \frac{1-k^{n+1}}{1-k} = \frac{1}{1-k}$$

but *divergent* otherwise.

One final interesting example: the 'harmonic' series

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots$$

is divergent! To see this, group the terms as follows

$$1 + \frac{1}{2} + (\frac{1}{3} + \frac{1}{4}) + (\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}) + \dots$$

It will be evident that the partial sums in brackets are greater than 1/2. Thus the sum is 'greater' than the sum of infinitely many 1/2s, which is greater than half the sum of infinitely many 1s, and hence infinite.

4.3 Introduction to difference equations

Suppose $a_1, a_2, \dots, a_n$ is a sequence. Define the *difference operator* Δ by

$$\Delta a_i = a_{i+1} - a_i.$$

(So $\Delta a_2 = a_3 - a_2$ and so on.)

We can use Δ repeatedly:

$$\Delta^2 a_i = \Delta(\Delta a_i) = \Delta(a_{i+1} - a_i) = a_{i+2} - 2a_{i+1} + a_i.$$

Just as an equation built using differential operators is called a differential equation, so equations built using Δ are called *difference equations*. For example

$$\Delta^2 a_i - 3\Delta a_i + 4a_i = 7$$

is a difference equation. Since we can expand this kind of equation to an equation involving a_i and a_{i+1} and so on, such equations are also difference equations. For example

$$a_{i+1} - 6a_i = 4.$$

Just as for differential equations, the problem is to solve for the sequence $\{a_i\}$ which obeys the equation for all i (possibly in terms of some initial values). Again as for differential equations, there is no universal method, but a number of powerful techniques. We will consider just a few of them here. Restricting (in this course) to *linear* equations. These are equations which can be written in the form

$$P(\Delta)a_i = k$$

where P is a polynomial and k any given number. For example, if $P(\Delta) = \Delta^2 + 3\Delta - 2$ and $k = 7$ we have

$$(\Delta^2 + 3\Delta - 2)a_i = \Delta^2 a_i + 3\Delta a_i - 2a_i = 7$$

Each such equation has a *homogeneous* version:

$$P(\Delta)a_i = 0.$$

Unlike for differential equations, one method which is open to us here is simply to insert values for the first few elements of the sequence as appropriate, and then do arithmetic to work out, using the equation, as many subsequent terms in the sequence as we might want. This *can* be very useful. On the other hand, a 'closed form' solution is one where we write the general element of the sequence as a function of the position i. This is *usually* what is required.

Consider the simple case

$$a_{i+1} - 2a_i = 0$$

Obviously $a_2 = 2a_1$, $a_3 = 2a_2$ and so on, so $a_i = 2^{i-1}a_1$. Any sequence of this form will satisfy the equation, so we can choose a_1 freely. (Sometimes this initial value is given in the problem.) Another way to look at this is to *guess* that the solution may take the form

$$a_i = kt^i.$$

Here k and t are constants which may be tuned so as to try to make the guess work. Here we find that k may take any value, while $t = 2$ is forced.

Note that if $a_i = f(i)$ is some solution to $P(\Delta)a_i = 0$ (i.e. $P(\Delta)f(i)$ is identically zero for all $i \in \mathbb{N}$), and $a_i = g(i)$ is some other solution, then $a_i = cf(i) + dg(i)$ is again a solution for any constants c, d. (This is why such equations are called *linear*.)

Similarly if $a_i = f(i)$ is some solution to $P(\Delta)a_i = 0$ and $a_i = g(i)$ is some solution to $P(\Delta)a_i = k$, then $a_i = f(i) + g(i)$ is again a solution to $P(\Delta)a_i = k$.

Now for

$$a_{i+1} - 2a_i = 2$$

one way to guess a particular solution is to try the guess $a_i = m$, where m is some constant (i.e. a solution in which the sequence is not varying!). If we plug this guess in we get $m - 2m = -m = 2$ i.e. $m = -2$. Thus $a_i = -2$ is a solution. (Note that this is easy to check.) Now if we ADD a solution to the associated *homogeneous* problem to this one (as it happens the previous problem is the homogeneous version of this one) we get another solution to this problem. Using this idea then, the general solution is $a_i = -2 + 2^{i-1}a_1$.

On the other hand we can also guess another particular solution, writing the equation as $a_{i+1} = 2 + 2a_i$: if we start with $a_1 = 0$ the sequence is determined as

$$0, 2, 6, 14, 30, \ldots$$

i.e. $a_i = 2^i - 2$. Altogether the general solution is then $a_i = 2^i - 2 + 2^{i-1}a_1$, where a_1 can be chosen freely. At first glance this looks different to the answer we got above. However this is the *same* as the general solution we had before — up to a different choice of a_1.

Now consider

$$a_{i+2} - 5a_{i+1} + 6a_i = 0.$$

Again we can make a guess like that above: $a_i = kc^i$. Substituting we get

$$kc^{i+2} - 5kc^{i+1} + 6kc^i = kc^i(c^2 - 5c + 6) = kc^i(c - 3)(c - 2) = 0$$

Putting aside the solution $kc = 0$ we have that either $c = 3$ of $c = 2$. (The factor $(c-3)(c-2)$ here is called the associated polynomial.) Both choices for c provide a solution for any k, thus we have that anything of the form

$$a_i = A2^i + B3^i$$

is a solution (any constants A, B).
NOTE, that it is easy to check this!

Exercise 24 *Solve* $a_{i+2} - 4a_{i+1} + 5a_i = 0$.
(Answer: The associated polynomial is $c^2 - 4c + 5$, with roots $c = 2 \pm i$. It is helpful to write $2 \pm i = D\exp(\pm i\theta)$ giving $D = \sqrt{5}$ and $\sin\theta = \frac{1}{\sqrt{5}}$ and $\cos\theta = \frac{2}{\sqrt{5}}$. Thus the general solution is $a_j = 5^{\frac{j}{2}}(A\cos r\theta + B\sin r\theta)$ where A, B are arbitrary constants.)