1.1 What is Algebra?

If you ask someone on the street this question, the most likely response will be: "Something horrible to do with x, y and z". If you're lucky enough to bump into a mathematician then you might get something along the lines of: "Algebra is the abstract encapsulation of our intuition for composition". By composition, we mean the concept of two object coming together to form a new one. For example adding two numbers, or composing real valued single variable functions. As we shall discover, the seemly simple idea of composition hides vast hidden depth.

Algebra permeates all of our mathematical intuitions. In fact the first mathematical concepts we ever encounter are the foundation of the subject. Let me summarize the first six to seven years of your mathematical education:

The concept of *Unity*. The number 1.
You probably always understood this, even as a little baby.

$\downarrow$

$\mathbb{N} := \{1, 2, 3...\}$, the natural numbers. $\mathbb{N}$ comes equipped with two natural operations $+$ and $\times$.

$\downarrow$

$\mathbb{Z} := \{... - 2, -1, 0, 1, 2, ...\}$, the integers.
We form these by using geometric intuition thinking of $\mathbb{N}$ as sitting on a line. $\mathbb{Z}$ also comes with $+$ and $\times$. Addition on $\mathbb{Z}$ has particularly good properties, e.g. additive inverses exist.

$\downarrow$

$\mathbb{Q} := \{\frac{a}{b} \,|a, b \in \mathbb{Z}, b \neq 0\}$, the rational numbers. We form these by taking $\mathbb{Z}$ and *formally* dividing through by non-negative integers. We can again use geometric insight to picture $\mathbb{Q}$ as points on a line. The rational numbers also come equipped with $+$ and $\times$. This time, multiplication is has particularly good properties, e.g non-zero elements have multiplicative inverses.

We could continue by going on to form $\mathbb{R}$, the real numbers and then $\mathbb{C}$, the complex numbers. This process is of course more complicated and steps into the realm of mathematical analysis.

Notice that at each stage the operations of $+$ and $\times$ gain additional properties. These ideas are very simple, but also profound. We spend years understanding how $+$ and $\times$ behave in $\mathbb{Q}$. For example

$$a + b = b + a \text{ for all } a, b \in \mathbb{Q},$$

or

$$a \times (b + c) = a \times b + a \times c \text{ for all } a, b, c \in \mathbb{Q}.$$

The central idea behind abstract algebra is to define a larger class of objects (sets with extra structure), of which $\mathbb{Z}$ and $\mathbb{Q}$ are definitive members.

$$\begin{aligned} (\mathbb{Z}, +) &\longrightarrow \textit{Groups} \\ (\mathbb{Z}, +, \times) &\longrightarrow \textit{Rings} \\ (\mathbb{Q}, +, \times) &\longrightarrow \textit{Fields} \end{aligned}$$

In linear algebra the analogous idea is

$$(\mathbb{R}^n, +, \text{scalar multiplication}) \longrightarrow \textit{Vector Spaces over } \mathbb{R}$$

The amazing thing is that these vague ideas mean something very precise and have far far more depth than one could ever imagine.

1.2 Sets and Functions

A set is any collection of objects. For example six dogs, all the protons on Earth, every thought you've ever had, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Observe that $\mathbb{Z}$ and $\mathbb{Q}$ are sets with extra structure coming from $+$ and $\times$. In this whole course, all we will study are sets with some carefully chosen extra structure.

Basic Logic and Set Notation

Writing mathematics is fundamentally no different than writing english. It is a language which has certain rules which must be followed to accurately express what we mean. Because mathematical arguments can be highly intricate it is necessary to use simplifying notation for frequently occurring concepts. I will try to keep these to a minimum, but it is crucial we all understand the following:

- If P and Q are two statements, then $P \Rightarrow Q$ means that if P is true then Q is true. For example: x odd $\Rightarrow x \neq 2$. We say that P implies Q.
- If $P \Rightarrow Q$ and $Q \Rightarrow P$ then we write $P \iff Q$, which should be read as P is true if and only if Q is true.
- The symbol $\forall$ should be read as "for all".
- The symbol $\exists$ should be read as "there exists". The symbol $\exists!$ should be read as "there exists unique".

Let S and T be two sets.

- If s is an object contained in S then we say that s is an *element*, or a *member* of S. In mathematical notation we write this as $s \in S$. For example $5 \in \mathbb{Z}$. Conversely $s \notin S$ means that x is not contained in S. For example $\frac{1}{2} \notin \mathbb{Z}$.
- If S has finitely many elements then we say it is a finite set. We denote its cardinality (or size) by $|S|$.
- The standard way of writing down a set S is using *curly bracket* notation.

  $$S = \{ \text{ Notation for elements in S } | \text{ Properties which specifies being in S } \}.$$

  The vertical bar should be read as "such that". For example, if S is the set of all even integer then

  $$S = \{x \in \mathbb{Z} \mid 2 \text{ divides } x\}.$$

  We can also use the curly bracket notation for finite sets without using the | symbol. For example, the set S which contains only 1,2 and 3 can be written as

  $$S = \{1, 2, 3\}.$$

- If every object in S is also an object in T, then we say that S is contained in T. In mathematical notation we write this as $S \subset T$. Note that $S \subset T$ and $T \subset S \Rightarrow S = T$. If S is *not* contained in T we write $S \not\subset T$.
- If $S \subset T$ then $T \setminus S := \{x \in T \mid x \notin S\}$. $T \setminus S$ is called the *compliment* of S in T.
- The set of objects contained in both S and T is call the intersection of S and T. In mathematical notation we denote this by $S \cap T$.
- The collection of all objects which are in either S or T is call the union on S and T. In mathematical notation we denote this by $S \cup T$.
- $S \times T = \{(a, b) | a \in S, b \in T\}$. We call this new set the (cartesian) product of S and T. We may naturally extend this concept to finite collections of sets.

- The set which contains no objects is called the empty set. We denote the empty set by $\emptyset$. We say that S and T are *disjoint* if $S \cap T = \emptyset$. The union of two disjoint sets is often written as $S \coprod T$.

Definition. *A map (or function) f from S to T is a rule which assigns to each element of S a unique elements of T. We express this information using the following notation:*

$$\begin{aligned} f : S &\to T \\ x &\mapsto f(x) \end{aligned}$$

Here are some examples of maps of sets:

1. $S = T = \mathbb{N}$,

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{N} \\ a &\mapsto a^2 \end{aligned}$$

2. $S = \mathbb{Z} \times \mathbb{Z}$, $T = \mathbb{Z}$,

$$\begin{aligned} f : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (a, b) &\mapsto a + b \end{aligned}$$

This very simple looking abstract concept hides enormous depth. To illustrate this, observe that calculus is just the study of certain classes of functions (continuous, differentiable or integrable) from $\mathbb{R}$ to $\mathbb{R}$.

Definition. *Let S and T be two sets,and $f : S \to T$ be a map.*

1. *We say that S is the domain of f and T is the codomain of f.*
2. *We say that f is the identity map if $S = T$ and $f(x) = x$, $\forall x \in S$. In this case we write $f = Id_S$.*
3. *f is injective if $f(x) = f(y) \Rightarrow x = y \; \forall \; x, y \in S$.*
4. *f is surjective if given $y \in T$, there exists $x \in S$ such that $f(x) = y$.*
5. *If f is both injective and surjective we say it is bijective. Intuitively this means f gives a perfect matching of elements in S and T.*

Observe that if R, S and T are sets and $g : R \to S$ and $f : S \to T$ are maps then we may compose them to give a new function: $f \circ g : R \to T$. Note that this is only possible if the domain of f is naturally contained in the codomain of g.

Important Exercise. *Let S and T be two sets. Let f be a map from S to T. Show that f is a bijection if and only if there exists a map g from T to S such that $f \circ g = Id_T$ and $g \circ f = Id_S$.*

1.3 Equivalence Relations

Within a set it is sometimes natural to talk about different elements being related in some way. For example, in $\mathbb{Z}$ we could say that $x, y \in \mathbb{Z}$ are related if $x - y$ is divisible by 2. Said another way, x and y are related is they are both odd or both even. This idea can be formalized as something called an *equivalence relation.*

Definition. *An equivalence relation on a set S is a subset $U \subset S \times S$ satisfying:*

1. $(x, y) \in U \iff (y, x) \in U$. *(This is called the symmetric property.)*
2. $\forall x \in S, (x, x) \in U$. *(This is called the reflexive property.)*
3. *Given $x, y, z \in S$, $(x, y) \in U$ and $(y, z) \in U \Rightarrow (x, z) \in U$. (This is called the transitive property.)*

If $U \subset S \times S$ is an equivalence relation then we say that $x, y \in S$ are *equivalent* if and only if $(x, y) \in U$. In more convenient notation, we write $x \sim y$ to mean that x and y are equivalent.

Definition. *Let $\sim$ be an equivalence relation on the set S. Let $x \in S$. The equivalence class containing x is the subset*

$$[x] := \{y \in S \mid y \sim x\} \subset S.$$

Remarks.

1. *Notice that the reflexive property implies that $x \in [x]$. Hence equivalence classes are non-empty and their union is S.*
2. *The symmetric and transitive properties imply that $y \in [x]$ if and only if $[y] = [x]$. Hence two equivalence classes are equal or disjoint. It should also be noted that we can represent a given equivalence class using any of its members using the $[x]$ notation.*

Definition. *Let S be a set. Let $\{X_i\}$ be a collection of subsets. We say that $\{X_i\}$ forms a partition of S if each X_i is non-empty, they are pairwise disjoint and their union is S.*

We've seen that the equivalence classes of an equivalence relation naturally form a partition of the set. Actually there is a converse: Any partition of a set naturally gives rise to an equivalence relation whose equivalence classes are the members of the partition. The conclusion of all this is that an equivalence relation on a set is the same as a partition. In the example given above, the equivalence classes are the odd integers and the even integers. **Equivalence relations and equivalence classes are incredibly important. They will the foundation of many concepts throughout the course. Take time to really internalize these ideas.**