2 Sets

Sets are an important mathematical concept for applications in computing, e.g. the information in a database can be described in terms of sets. Many of the mathematical techniques that we will learn later in this module are formulated in terms of sets. This section will cover the most important concepts and techniques from set theory.

2.1 Basic Concepts and Notations

A *set* is a collection of items, which are called its *elements*. Almost any kind of item is allowed and their ordering is not important. Two sets are equal if and only if they contain the same elements.

Example 2.1 *The following are examples of sets:*

1. *All current DCU students.*
2. *The primary colours.*
3. *The natural numbers from 1 to 100.*

There are several ways to write sets. We always write the elements of the set in curly braces. If there are only few elements we can list them explicitly, e.g.

$$\{1,2,3,4,5,6,7,8,9,0\},$$
$$\{\text{red, green, blue}\}.$$

Alternatively, we can write a set in terms of a description and a condition that its elements satisfy. The condition is stated after a symbol "|" (or ":" in some books), e.g.

$$\{x \text{ a real number} \mid x^2 = 1\}.$$

Note that the condition takes the form of a predicate $P(x)$ with domain of discourse D, so in general this notation takes the form $\{x \in D \mid P(x)\}$. Finally, we can give a set a name, e.g. $A = \{-1, 0, 1\}$.

Example 2.2 *A single set can often be written in different ways, e.g.*

$$\{x \textit{ a real number} \mid x^2 = 1\} = \{-1, 1\} = \{1, -1\}.$$

There is a unique set which has no elements, the *empty set*, which is denoted by $\varnothing$. Sets can also contain other sets as an element, e.g. $\{\{1,2\},2,3,\{1,2,3,4\}\}$. Note that $\{\varnothing\}$ is not the empty set, but a set with a single element, which is $\varnothing$.

For any x and any set A we write $x \in A$ when A contains x as an element and $x \notin A$ when this is not the case. Note that for a fixed x the formula $x \in A$ is a proposition: it is either true or false, but not both. $x \notin A$ is another notation for $\neg(x \in A)$. When the identity of x is unknown, $x \in A$ is a predicate.

Remark 2.3 *Sets can contain many kinds of items, including other sets, but there are things which are not allowed. Consider the following description:*

A is the collection of all sets which do not contain themselves as an element, i.e.
$$A = \{B \textit{ a set} \mid B \notin B\}.$$

If A were a set, then we could ask for the truth value of $A \in A$. One can check that this statement can be neither true nor false, because both options contradict the definition of A. This is called Russel's paradox. If we insist that $A \in A$ is a proposition for every set A, then the description above does not define a set. The paradox can be avoided by imposing additional requirements on the description of sets (see e.g. [3]), but we will not consider those in this module.

2.2 Standard Sets of Numbers and Arithmetic Operations

We briefly review the main sets of numbers and their arithmetic operations.

Natural numbers: The set of natural numbers is $\mathbb{N} = \{1, 2, 3, \ldots\}$. It contains infinitely many numbers (but "infinity" is not a number itself). We say that $\mathbb{N}$ is closed under addition and multiplication, i.e., for any $m \in \mathbb{N}$ and $m \in \mathbb{N}$ there are unique numbers $m + n$ and $m \cdot n$ which are again in $\mathbb{N}$. The natural numbers are not closed under subtraction, e.g. $2 - 5$ is not a natural number, even though 2 and 5 are.

Integers: The set of integers is $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. It contains $\mathbb{N}$, but also 0 and the negatives of all natural numbers. $\mathbb{Z}$ is closed under addition and multiplication and also under subtraction.The natural numbers are not closed under subtraction. $\mathbb{Z}$ is not closed under division, e.g. $\frac{2}{5}$ is not an integer, even though 2 and 5 are.

Rational numbers: The set of rational numbers is $\mathbb{Q} = \{\frac{m}{n} | \ m \in \mathbb{Z}, n \in \mathbb{N}\}$, where we identify two numbers $\frac{m}{n}$ and $\frac{p}{q}$ if and only if $q \cdot m = n \cdot p$, e.g. $\frac{2}{4} = \frac{1}{2}$. We also identify $\frac{m}{1}$ with m, so $\mathbb{Q}$ contains $\mathbb{Z}$. $\mathbb{Q}$ is closed under addition, multiplication, subtraction and under division by non-zero numbers. More explicitly we have for any rational numbers $\frac{m}{n}$ and $\frac{p}{q}$ we have

$$\begin{aligned}
\frac{m}{n} \cdot \frac{p}{q} &= \frac{m \cdot p}{n \cdot q} \\
\frac{m}{n} + \frac{p}{q} &= \frac{m \cdot q}{n \cdot q} + \frac{n \cdot p}{n \cdot q} = \frac{m \cdot q + n \cdot p}{n \cdot q} \\
-\frac{m}{n} &= \frac{-m}{n} \\
\frac{m}{n} \div \frac{p}{q} &= \frac{m}{n} \cdot \frac{q}{p} = \frac{m \cdot q}{n \cdot p}
\end{aligned}$$

where $p \neq 0$ in the last line. When it comes to addition, multiplication, subtraction and division, $\mathbb{Q}$ is as good as it gets.

Real numbers: The set of real numbers $\mathbb{R}$ contains all numbers on the number line, including all rational numbers, but also $\sqrt{2}$, π, e and many others. (Such real numbers which are not rational are called irrational.) More precisely, the real numbers are those numbers that can be obtained from numbers in $\mathbb{Q}$ by taking limits, but this topic is beyond the scope of this module. It is important to know that the rules of computation for rational numbers extend to real numbers, so $\mathbb{R}$ is still as good as it gets when it comes to addition, multiplication, subtraction and division. Furthermore, it is closed under taking limits. However, there is no real number x such that $x^2 = -1$, so we cannot always take square roots.

Complex numbers: The set of complex numbers are all numbers of the form $x + i \cdot y$, where x and y are real numbers and i is a number such that $i^2 = -1$. i is not real, so it cannot be pictured on the number line. Instead, we picture the complex numbers in a two-dimensional plane. $\mathbb{C}$ is closed under limits and all rules of computation still hold. $\mathbb{C}$ has some very nice additional properties, but we will rarely use it in this module.

2.3 Subsets and Venn Diagrams

A *subset* A of a set B is a set such that every element of A is also an element of B, i.e. $(x \in A) \Rightarrow (x \in B)$. In this case we write $A \subseteq B$ or $B \supseteq A$ and we call B a *superset* of A. When A is not a subset of B we write $A \nsubseteq B$ or $B \nsupseteq A$.

Two sets A and B are *equal*, written $A = B$, if and only if both $A \subseteq B$ and $B \subseteq A$. This shows that the ordering of the elements of a set is unimportant. We call A a *proper subset* of

B when $A \subseteq B$, but $A \neq B$ (i.e, $\neg(A = B)$). In this case B is a *proper superset* if A and we write $A \subsetneq B$ and $B \supsetneq A$.

A convenient way to depict sets and their relations is in *Venn diagram.* In such a diagram, a set is represented by an oval and we imagine all its elements are inside it. Elements can be depicted by points, but they are often omitted, especially when sets have infinitely many elements. E.g., the Venn diagram in Figure 1 depicts the inclusions $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

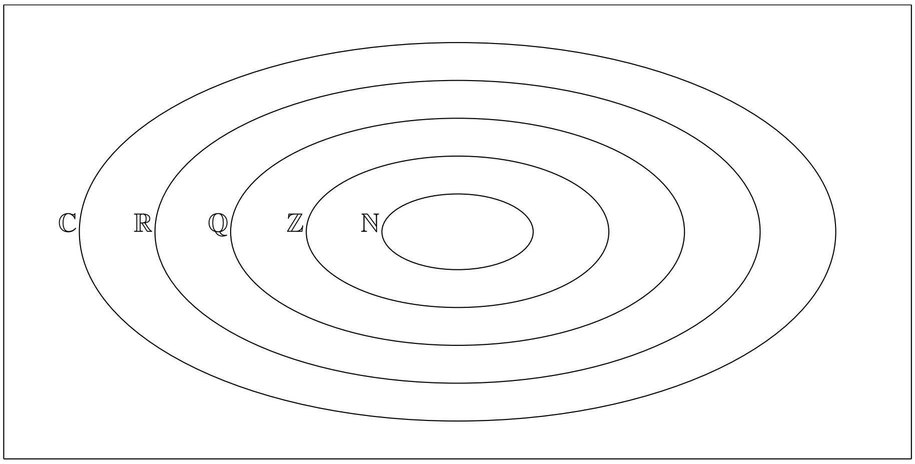

Figure 1: A Venn diagram depicting the inclusions between the standard sets of numbers.

The box surrounding the Venn diagram in Figure 1 can also be thought of as set which contains all the sets and all elements relevant to the situation. We call this set the *universal set* for this situation and we denote it by U. A universal set in set theory is a bit analogous to the domain of discourse in logic. In particular, the universal set may vary from one problem to the next. For problems about numbers we can often take U to be $\mathbb{R}$ or $\mathbb{C}$.

For any set A we define the *power set* $\mathcal{P}(A)$ to be the set of all subsets of A. The power set $\mathcal{P}(A)$ always contains $\varnothing$ and A as elements. When $A = \varnothing$ we have $\mathcal{P}(\varnothing) = \{\varnothing\}$.

Example 2.4 *The set* $A = \{1, 2, 3\}$ *has power set*

$$\mathcal{P}(A) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}.$$

2.4 Set Operations

We can construct new sets from given sets, much in analogy to the way in which we combine propositions to obtain new ones. Here are the main constructions, which are also depicted in Figure 2.

Intersection: The intersection of two sets A and B is the set $A \cup B$ consisting of all items that are elements of A and of B, i.e. $x \in A \cap B$ if and only if $(x \in A) \wedge (x \in B)$. When $A \cap B = \varnothing$ we call the sets A and B *disjoint.*

Union: The union of two sets A and B is the set $A \cap B$ consisting of all items that are elements of A or of B (or both), i.e. $x \in A \cup B$ if and only if $(x \in A) \vee (x \in B)$.

Complement: The complement of a set A, written as A^c, depends on the choice of a universal set $U \supseteq A$. Given U, the complement of A consists of all elements in U that are not in A, i.e. $x \in A^c$ if and only if $\neg(x \in A)$ and $x \in U$.

Warning: The notation A^c for the complement of A does not show that it depends on the choice of a universal set U. Although this is an unfortunate drawback of the notation, it is nevertheless standard to use it.

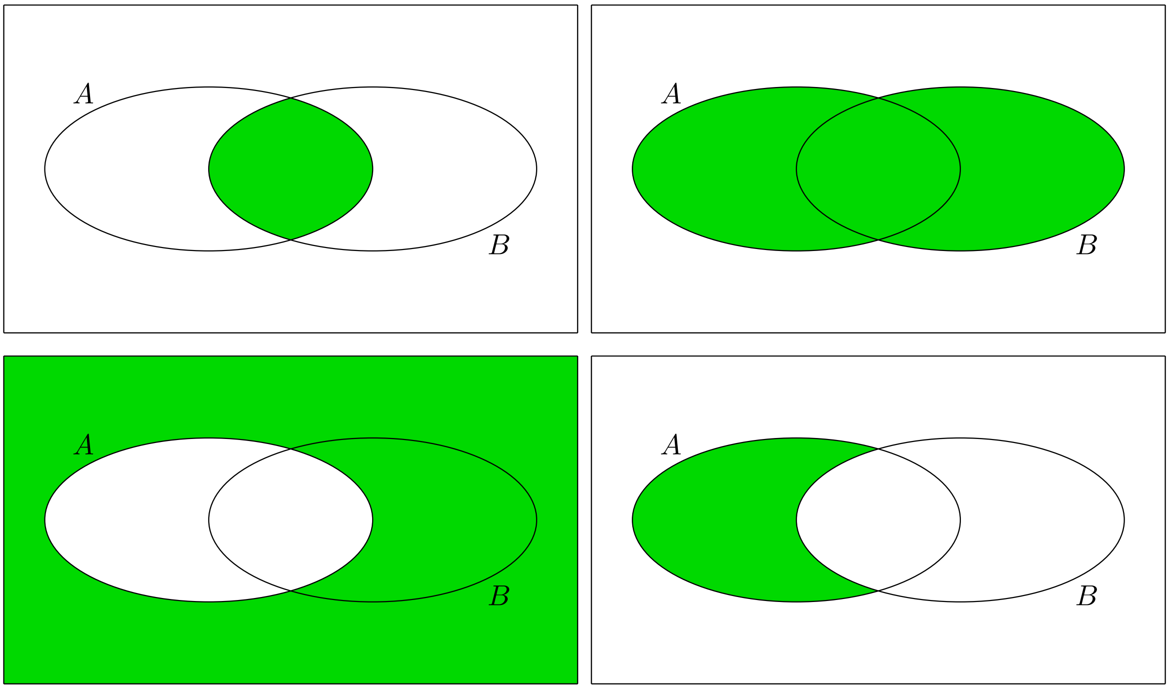

Figure 2: Venn diagrams depicting the sets $A \cap B$, $A \cup B$, A^c (w.r.t. the universal set) and $A \setminus B$.

Difference: The difference of a set A minus a set B, written as $A \setminus B$, is the set of all elements in A that are not in B, i.e. $x \in A \setminus B$ if and only if $(x \in A) \wedge (\neg(x \in B))$. Note that the complement is also a set difference, $A^c = U \setminus A$. In general, B need not be a subset of A, however.

set	expression
$A^c =$	$\{x \in U \mid \neg(x \in A)\}$
$A \cap B =$	$\{x \in U \mid (x \in A) \wedge (x \in B)\}$
$A \cup B =$	$\{x \in U \mid (x \in A) \vee (x \in B)\}$

Table 3: The relation between some set operations and logical connectives for sets A and B in a universal set U.

Note that the set operations are essentially defined in terms of the logical connectives $\wedge$, $\vee$ and $\neg$ and the choice of a universal set U. Table 3 gives an overview. As a consequence, the logical rules for $\wedge$, $\vee$ and $\neg$ also give rise to identities for rewriting formulae for sets involving $\cap$, $\cup$ and ^{c}. Some of the most important identities have names that are very similar to their logical counterparts. They are listed in Table 4.

It is instructive to show De Morgan's law $(A \cap B)^c = A^c \cup B^c$. This can be derived directly from the corresponding law in propositional logic, but we will instead use a truth table to derive that logical statement for the case at hand.

Let a be an arbitrary, but fixed, element in the universal set U and let p be the proposition $a \in A$ and q the proposition $a \in B$. We construct a truth table to show the equivalence of $\neg(p \wedge q)$ and $(\neg p) \vee (\neg q)$ (De Morgan's law in propositional logic).

set identity	name of rule
$(A \cap B)^c = A^c \cup B^c$	De Morgan's law
$(A \cup B)^c = A^c \cap B^c$	De Morgan's law
$(A^c)^c = A$	double complement law
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	distributive law of $\cap$ over $\cup$
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	distributive law of $\cup$ over $\cap$

Table 4: Some identites for sets involving set operations.

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

Note that each row of the truth table corresponds to a region in a Venn diagram, specifying whether we are inside or outside A and inside or outside B. The fourth and last columns have equal entries in every row, proving the desired equivalence. This means that $\neg((a \in A) \wedge (a \in B))$ is equivalent to $(\neg(a \in A)) \vee (\neg(a \in B))$. Using the definition of intersections, complements and unions this means that $a \in (A \cap B)^c$ if and only if $a \in A^c \cup B^c$. Since $a \in U$ was arbitrary we can use a universal generalization to deduce that $(A \cap B)^c = A^c \cup B^c$.

Example 2.5 *Not all set operations are independent of each other. E.g., the set difference $A \setminus B$ equals $A \cap B^c$, because $A \cap B^c = \{x \in U | \ (x \in A) \wedge (x \in B^c)\} = \{x \in U | \ (x \in A) \wedge \neg(x \in B)\}$. This identity can be visualised using a Venn diagram and proved using a truth table.*

Example 2.6 *We can extend Table 3 and use the connectives $\Rightarrow$ and $\Leftrightarrow$ to construct further sets from A and B, namely $\{x \in U | \ (x \in A) \Rightarrow (x \in B)\}$ and $\{x \in U | \ (x \in A) \Leftrightarrow (x \in B)\}$. Because $p \Rightarrow q$ is equivalent to $(\neg p) \vee q$ and $p \Leftrightarrow q$ is equivalent to $(p \Rightarrow q) \wedge (q \Rightarrow p)$ we find that*

$$\begin{aligned} &\{x \in U | \ (x \in A) \Rightarrow (x \in B)\} = \{x \in U | \ \neg(x \in A) \vee (x \in B)\} = A^c \cup B \,, \\ &\{x \in U | \ (x \in A) \Leftrightarrow (x \in B)\} = (A^c \cup B) \cap (A \cup B^c) \,. \end{aligned}$$

Note that we can also write $A^c \cup B = (A \cap B^c)^c = (A \setminus B)^c$.

2.5 Cardinality

A set A is called finite if it has finitely many elements in it. In this case the *cardinality* of A is the number of elements, which we write symbolically as $|A|$. E.g. $|\{\text{red, green, blue}\}| = 3$ and $|\{1, 2, 3, 4, 5\}| = 5$. (We will not consider the cardinality of sets with infinitely many elements.)

When $B \subseteq A$ and A has finitely many elements, then so does B and we have $|B| \leq |A|$. Indeed, we can often determine $|A|$ in terms of the cardinality of suitable subsets.

Definition 2.7 *A* partition *of a set A is a set of subsets of A such that every $x \in A$ is contained in exactly one of the subsets.*

When $\{A_1, A_2, \ldots, A_k\}$ is a partition of A into k sets, then $A = A_1 \cup A_2 \cup \ldots \cup A_k$ and $A_i \cap A_j = \varnothing$ when $i \neq j$. In this case we have

$$|A| = |A_1| + |A_2| + \ldots + |A_k| \,. \tag{1}$$

This can be shown by induction over the number k of sets in the partition. Alternatively, note that each element x in A is in exactly one of the A_i on the right-hand side, so it contributes 1 to the left-hand side and 1 to the right-hand side of the equality.

When $A \cap B = \varnothing$, then we can partition $A \cup B$ using $\{A, B\}$ and we find

$$|A \cup B| = |A| + |B|, \qquad (A \cap B = \varnothing).$$

The following proposition extends this identity to situations where A and B are not necessarily disjoint. Intuitively, if we add $|A|$ and $|B|$ we have counted all elements in $A \cup B$, but the elements in $A \cap B$ were counted twice. To correct for this error we need to subtract $|A \cap B|$.

Proposition 2.8 *For any finite sets A and B we have $|A \cup B| = |A| + |B| - |A \cap B|$.*

Proof: We can partition $A \cup B$ using $\{A, B \smallsetminus A\}$ and B using $\{B \smallsetminus A, B \cap A\}$. Applying Equation (1) yields $|A \cup B| = |A| + |B \smallsetminus A|$ and $|B| = |B \smallsetminus A| + |A \cap B|$. We can combine these equalities to

$$|A \cup B| = |A| + |B| - |A \cap B|$$

as was to be shown. □

This result can be generalised to a so-called inclusion-exclusion principle which deals with unions of arbitrarily many sets. It can be proved by mathematical induction over the number of sets, but the notation gets inreasingly cumbersome and we will not use it in this generality. However, we will consider the case of three sets.

Proposition 2.9 *For any finite sets A, B and C we have*

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Proof: We write $A \cup B \cup C = (A \cup B) \cup C$ and use Proposition 2.8 twice to get

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

Now we note that $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ and we get from Proposition 2.8

$$|(A \cup B) \cap C| = |(A \cap C) \cup (B \cap C)| = |A \cap C| + |B \cap C| - |A \cap B \cap C|,$$

because $(A \cap C) \cap (B \cap C) = A \cap B \cap C$. We can substitute this into the previous equation and reorder the terms to get the formula in the statement of the proposition, as was to be shown. □

Example 2.10 *A group of 73 students is asked whether they speak French, German or Spanish. All students speak at least one of these foreign language. 45 speak French, 33 speak German, 27 speak Spanish, 13 speak French and German, 11 speak French and Spanish and 10 speak German and Spanish. How many students speak French, German and Spanish?*

Solution: *Let F be the set of students who speak French, G the set of students who speak German and S the set of students who speak Spanish. Because all students speak at least one of these languages we have $|F \cup G \cup S| = 73$. We also have $|F| = 45$, $|G| = 33$, $|S| = 27$, $|F \cap G| = 13$, $|F \cap S| = 11$ and $|G \cap S| = 10$. By Proposition 2.9 this means that $73 = 45 + 33 + 27 - 13 - 11 - 10 + |F \cap G \cap S|$. It follows that $|F \cap G \cap S| = 73 - 45 - 33 - 27 + 13 + 11 + 10 = 2$.*

We can also find the cardinality of a power set in terms of the cardinality of the original set.

Theorem 2.11 *Let A be a finite set, then $|\mathcal{P}(A)| = 2^{|A|}$.*

Proof: When $A = \varnothing$ then $|A| = 0$ and $\mathcal{P}(A) = \{\varnothing\}$ has a single element, so $|\mathcal{P}(A)| = 1 = 2^0$, as desired. When $A \neq \varnothing$ we introduce $n = |A|$, which is a natural number, and we give a proof by mathematical induction.

In the base case A has a single element, which we call x_1. To find a subset of A we need to decide if x is in it or not. This gives two possibilities, namely $\{x\} = A$ and $\varnothing$. Therefore, $|\mathcal{P}(A)| = 2 = 2^1$. This proves the base case.

For the induction step we assume that the statement is true for all sets with cardinality n for some $n \in \mathbb{N}$. Now suppose that $|A| = n + 1$ and let $x_1 \in A$ be an element. We introduce $B = A \smallsetminus \{x_1\}$ so that $A = \{x_1\} \cup B$. We now divide the subsets of A into two disjoint sets. If a subset of A does not contain x_1, then it is also a subset of B. From the induction hypothesis we know that there are 2^n of such subsets. Alternatively, if a subset of A does contain x_1, then it is of the form $\{x_1\} \cup C$ for some subset $C \subset B$. Again there are 2^n different choices of C, so in total the number of subsets of A is $2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$, which proves the induction step. By the principle of mathematical induction we find that $|\mathcal{P}(A)| = 2^{|A|}$ for any value of $|A|$, as was to be shown. □

2.6 Cartesian Products

There is one more way to obtain new sets from given ones which will be important in the remainder of this module. The *Cartesian product* of two sets, A and B, is the set consisting of pairs of elements, one from each set. We write this product as $A \times B$, so

$$A \times B = \{(a,b) | \ (a \in A) \wedge (b \in B)\} .$$

Here (a,b) is a pair of elements, one from A and one from B. Note that (a,b) is not written as a set: it has (round) parentheses rather than curly braces. Note in particular that the ordering of A and B and the ordering of the elements matters: to get an element (a,b) of $A \times B$ we need $a \in A$ and $b \in B$, not $a \in B$ and $b \in A$. It is also possible to take a Cartesian product of more than one set, e.g.

$$A \times B \times C = \{(a,b,c) | \ (a \in A) \wedge (b \in B) \wedge (c \in C)\}$$

etc.

Example 2.12 1. *The Cartesian product of the sets $A = \{$red, green$\}$ and $B = \{$triangle, circle$\}$ is $A \times B = \{($red,triangle$), ($red,circle$), ($green,triangle$), ($green,circle$)\}$.*

2. *A byte consists of 8 bits, each of which can take a value in $\{0,1\}$. We can identify a byte with an element of the eight-fold Cartesian product $\{0,1\} \times \{0,1\} \times \ldots \times \{0,1\} = \{0,1\}^{\times 8}$, where we identify e.g.* 01100010 *with the element* $(0,1,1,0,0,0,1,0)$.

3. *We can speficy a point in the plane by giving two coordinates, (x,y), which are both real numbers. This means that we can identify the plan with $\mathbb{R} \times \mathbb{R}$ in much the same way as we identify $\mathbb{R}$ with the number line.*

If the sets A and B are finite, then so is the Cartesian product $A \times B$ and we have $|A \times B| = |A| \cdot |B|$.