Math 4055 Background Notes

Ambar N. Sengupta
Department of Mathematics
Louisiana State University, Baton Rouge

February, 2002

Chapter 1

Set Theory

Set theory is both a branch of mathematics and, along with logic, the foundation for mathematics. It is the structure on which all of mathematics rests and provides the language in which practically all of mathematics is written. Virtually every object in mathematics is a set.

Set theory has no applications in daily life, nor does it have any direct application to the sciences. However, it is the foundation for all of mathematics and thus, indirectly, provides the solid ground on which an enormous amount of science, engineering, statistics and finance rests.

No one invented set theory with the intention of providing the foundation for mathematics, let alone for any concrete applications in science or daily life. Set theory was invented by Georg Cantor in the 1860s as a systematic framework in which he could formulate his abstruse investigations of infinite numbers. His ideas were considered too esoteric then and few of the great minds of that era recognized that Cantor had invented an amazingly versatile language which could be used to formulate virtually every mathematical concept in a precise way. Cantor's theory eventually led to the development of mathematical logic and then this led much later, in the twentieth century, through the works of Gödel and Turing, to the idea of a machine which could execute commands without needing to "understand" (in human intuitive terms) what the commands meant. Eventually, such a machine was indeed built and today we know it as the computer.

Most working mathematicians today view set theory as an enormously useful language in which they write their works. But many consider investigation of set theory in itself an abstruse endeavor. However, set theory is in fact still very much an active area of research with many deep questions.

1.1 Sets

A <u>set</u> is a collection of objects. These objects are called <u>elements</u> of the set.

We often write a set by displaying its elements within braces. For example,

$$\{a, b, c\}$$

is the set whose elements are a, b, and c.

It is important to note that the set $\{a, b, c\}$ is the same as the set $\{b, c, a\}$; these being just two different ways of displaying the same set. Similarly, $\{a, b, b\}$ is the same set as $\{a, b\}$, since both sets really have the exact same elements a and b.

A set x is said to be <u>equal</u> to a set y, written $x = y$, if x and y have exactly the same elements. For example,

$$\{a, a, b, b, c\} = \{b, a, c\}$$

because both sets have exactly the same elements: a, b, and c.

To prove that two sets are not equal we need only *produce an object which is an element of one set but not an element of the other.*

The statement " x is an element of y" is written symbolically as:

$$x \in y$$

For example,

$$a \in \{a, b\}$$

The simplest set of all is the <u>empty set</u>, denoted $\emptyset$. This set has no elements at all. Thus, using the braces notation to specify the empty set,

$$\emptyset = \{\ \}$$

It is an amazing fact that *virtually every object in mathematics can be constructed out of the empty set* using certain simple steps!

Question. Is $\emptyset \in \emptyset$?

Answer. No. Because $\emptyset$ contains no element at all. So, in particular, it certainly does not contain $\emptyset$ as an element. ♣

1.2 The first sets: $\emptyset$ and 1

Starting with the empty set $\emptyset$ we can creat a new set

$$\{\emptyset\}$$

This is the set with exactly one element, that element being $\emptyset$. It is important to understand that $\{\emptyset\}$ is *not* the empty set, for it does contain an element, that being $\emptyset$.

The set $\{\emptyset\}$ is the first set we have constructed and contains one elements. This set has the name 1:

$$1 = \{\emptyset\} \tag{1.1}$$

In mathematics, one picks out certain statements of importance and interest and calls them "theorems." A theorem must, of course, be true and so a formal *proof* is needed. A proof is a *completely logical argument*. You cannot prove a general claim by simply giving an example illustrating the claim or by saying "it looks obvious." It is not always easy to read and understand mathematical proofs since they are written in a strictly logical and often terse manner. It is usually even more difficult to write down a proof. Read the proofs given in this text carefully and then, when needed, try formulating your own proofs.

As our first theorem, we state officially:

Theorem 1 *The sets $\emptyset$ and 1 are not equal to each other:*

$$\emptyset \neq 1$$

We have already seen why this is, but let us state the argument again in official form for the record:

Proof. For two sets to be equal they must contain exactly the same elements. Now 1 contains an element (namely, $\emptyset$), while $\emptyset$ contains no element at all. Hence, 1 is not equal to $\emptyset$. QED

1.3 The numbers $\emptyset, 1, 2, 3, ...$

We now have two sets

$$\emptyset \qquad \text{and} \qquad 1$$

Thus we can put these together and form another set

$$\{\emptyset, 1\}$$

Now this set contains two distinct elements $\emptyset$ and 1. In contrast, recall that the set $\emptyset$ contains no element at all while 1 contains just one element. Thus $\{\emptyset, 1\}$ is truly a new set. We give it the name 2:

$$2 = \{\emptyset, 1\} \tag{1.2}$$

As we have already observed, this set is neither equal to $\emptyset$ nor is it equal to 1. (One could state this observation formally as a theorem.)

Thus, now we have three distinct sets:

$$\emptyset, \qquad 1, \qquad \text{and} \qquad 2$$

Putting these sets together in one set we obtain a set

$$\{\emptyset, 1, 2\}$$

Needless to say, this is a new set again, and, of course, we call it 3:

$$3 = \{\emptyset, 1, 2\}$$

The process is now clear. We can continue to create new sets in this way. Endlessly:

$$\emptyset, 1, 2, 3, 4, 5, ...$$

We all understand intuitively what numbers are. But what set theory has done for us is provide precise and exactly defined objects which codify our intuitive notion of numbers.

When thought of as a number, the empty set $\emptyset$ is written as zero: 0.

1.4 Infinities

Now that we have all the familiar numbers

$$\emptyset, 1, 2, 3, 4, 5, ...$$

we can put them all together into one set

$$\omega_0 = \{\emptyset, 1, 2, 3, 4, 5, ...\}$$

This is a new number, it is an infinite number. It was constructed first by Georg Cantor in the 1860s and is called the first ordinal infinity.

Having constructed ω_0, there is no stopping us: we have then another number

$$\{\omega_0, \emptyset, 1, 2, 3, 4, 5, ...\}$$

This is another infinite ordinal number.

In this way, Cantor produced a vast array of infinite numbers and showed how to do arithmetic with them.

The term "ordinal" calls for some explanation. Although we all understand numbers intuitively, a little thought shows that there are actually two different senses in which we think of numbers: (i) as a counting tool (for instance, when we say $\{\emptyset, 1, 2\}$ contains three elements), and (ii) to order things, as in first, second, third,... . Cantor found that this distinction, more conceptual than literal when we deal with finite numbers, becomes a very real distinction when one deals with infinite numbers. Thus, in the world of infinite numbers there are actually two distinct types of numbers, the ordinals (used to order objects) and cardinals (used to count objects).

1.5 The integers, the rational numbers, and the real numbers

In ordinary mathematics one needs more than just the numbers $\emptyset, 1, 2, ...$ One uses also negative numbers $-1, -2, -3, ...$ Together these form the set of all integers

$$\{0, 1, -1, 2, -2, 3, -3, ...\}$$

This set is denoted by $\mathbf{Z}$:

$$\mathbf{Z} = \{0, 1, -1, 2, -2, 3, -3, ...\} \tag{1.3}$$

When we throw in all fractional numbers as well, we get the set of all rational numbers $\mathbf{Q}$. This set contains, in addition to all the integers, also numbers of the type $3/4$ and $-214/151$.

Thus the elements of $\mathbf{Q}$ are all numbers which can be written as a *ratio*

$$p/q$$

where p and q are integers. (One can't divide by 0, and so, of course, we can't have $q = 0$ here.)

There is a way to express this in mathematical language

$$\mathbf{Q} = \{p/q \qquad | \qquad p, q \in \mathbf{Z},\ q \neq 0\}$$

which we read as: "the set of all ratios p/q, with p, q being elements of $\mathbf{Z}$ and with q not equal to 0."

This descriptive way of specifying a set is very convenient and will be used often.

Thus, we have the basic sets of numbers:

$$\omega_0 = \{0, 1, 2, 3, ...\}, \quad \mathbf{Z} = \{0, 1, -1, 2, -2, 3, -3, ...\}, \quad \mathbf{Q} = \left\{ \frac{p}{q} \,\middle|\, p, q \in \mathbf{Z},\ q \neq 0 \right\}$$

The set $\{1, 2, 3, 4, ...\}$ is often called the set of all <u>natural numbers</u>, and is denoted by $\mathbf{N}$:

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

For most uses of mathematics it turns out that even the large set $\mathbf{Q}$ of all rational numbers is not large enough. For example, suppose you walk 1 mile east and then 1 mile to the north, on a flat plane. How far are you from where you started? Let us say it is X miles. According to Pythagoras' theorem, X^2 is equal to 2 (this comes from $1^2 + 1^2 = 2$). Now *it can be proven that there is no rational number whose square is* 2! Thus X cannot be an element of $\mathbf{Q}$. Thus the set $\mathbf{Q}$, though pretty large, is not large enough for the purposes of measuring lengths, for instance.

It is possible to enlarge $\mathbf{Q}$ into a big set $\mathbf{R}$, called the set of all <u>real numbers</u>, which does indeed contain a number whose square is 2. Indeed, $\mathbf{R}$ contains pretty much every number you can think of. For example, $\pi = 3.14159265....$ is an element of $\mathbf{R}$.

A crucial property of $\mathbf{R}$ is that if you take any positive number, say for example 15263.21458, there is an element in $\mathbf{R}$ whose square is the given number.

However, there is no real number whose square is -1. In other words, -1 has no square-root among the real numbers. Put another way, there is no way to solve the equation

$$x^2 = -1$$

if we wish to stick with real numbers.

In more advanced mathematics it is necessary to enlarge $\mathbf{R}$ to an even larger set $\mathbf{C}$, called the set of <u>complex numbers</u>. Here, even -1 has a square-root. The amazing fact about $\mathbf{C}$ is that even incredibly complicated equation

have solutions which are complex numbers. For example, even for the equation

$$x^{511} - 32x^{76} + 23x^3 = -\frac{211}{341}$$

it can be proven that there is indeed a number $x \in \mathbf{C}$ for which this equation is valid.

1.6 Subsets

Consider sets a and b. We say that a is a <u>subset</u> of b if every element of a is an element of b. We write

$$a \subset b$$

to mean a is a subset of b.

For example, consider the sets $x = \{0, 1\}$, $y = \{1, 2\}$, $z = \{0, 1, 2\}$. Then

$$x \subset z$$

and

$$y \subset z$$

On the other hand,

$$y \not\subset x$$

for y contains the element 2 which is not an element of x.

It is worth noting that $c \not\subset d$, i.e. c is not a subset of d, means that c contains some element which is not element of d.

A slightly surprising, but in truth almost obvious, fact is that every set is a subset of itself. Mathematically,

$$a \subset a$$

for every set a. The reason is simple: clearly, each element of a is an element of a!

Another observation is:

$$\text{if } a \subset b \text{ and } b \subset a \text{ then } a = b \tag{1.4}$$

Let us prove this formally:

Proof of (1.4) . Since $a \subset b$ every element of a is an element of b. On the other hand, since $b \subset a$, every element of b is an element of a. Thus, a and b have exactly the same elements. Therefore, $a = b$. QED

Another simple observation is

$$\text{if } a \subset b \text{ and } b \subset c \text{ then } a \subset c \tag{1.5}$$

Try to write out a formal proof of this.

Next we come to a fact which may seem a bit strange:

Theorem 2 *The empty set $\emptyset$ is a subset of every set.*

The proof of this is going to be our first example of a "proof by contradiction." This method may be difficult to accept if you are seeing this for the first time.

Proof. Consider any set a. We claim that $\emptyset$ is a subset of a. If this were not true, i.e. if $\emptyset$ were not a subset of a, then $\emptyset$ would have to have some element which is not an element of a. But this can't be true since $\emptyset$ has no element at all. Thus $\emptyset$ is indeed a subset of a. QED

The <u>power set</u> of a set x is the set of all subsets of x. It is denoted $\mathcal{P}(x)$.

For example, the empty set $\emptyset$ has just one subset, that being $\emptyset$ iself. So

$$\mathcal{P}(\emptyset) = \{\emptyset\}$$

The subsets of $\{1, 2\}$ are $\emptyset$ (which is a subset of *every set*), $\{1\}$, $\{2\}$, and $\{1, 2\}$ itself. Thus:

$$\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$$

Warning: In finding what the power set of a given set x is, it is very easy to forget that $\emptyset$ is a subset of x and also that x itself is a subset of x.

HOMEWORK

1. Write out a formal proof showing that $1 \neq 2$. (Recall that $1 = \{\emptyset\}$ and $2 = \{\emptyset, 1\}$.)

2. Explain clearly which of the following statements is/are true and which false: (a) $1 \in \emptyset$, (b) $2 \in 1$, (c) $1 \in 2$, (d) $\emptyset \in \emptyset$.

3. Among the sets $\omega_0, \mathbf{Z}, \mathbf{Q}, \mathbf{R}$, state which is a subset of which set.

4. Let $X = \{a, b, c\}$, where a, b, c are three distinct objects. Write out the power set $\mathcal{P}(X)$. How many subsets does X have?

5. Let $Y = \{a, b, c\}$, where a, b, c, d are four distinct objects. Write out the power set $\mathcal{P}(Y)$. How many subsets does Y have?

1.7 Unions and Intersections

Consider sets a and b. The union of these sets is the set formed by pooling together their elements into one set. The union of a and b is denoted

$$a \cup b$$

For example, suppose $x = \{1, 2, 3\}$ and $y = \{2, 3, 4, 0\}$. Then

$$x \cup y = \{1, 2, 3, 4, 0\}$$

(Note that there is no need to repeat 2 and 3.)

The intersection of sets a and b is the set of all elements which belong to both a and b. The intersection of a and b is denoted

$$a \cap b$$

If x and y being the sets mentioned above, then their intersection is

$$x \cap y = \{2, 3\}$$

Here are some basic facts about unions:

Theorem 3 *For any sets a, b, c,*

$$a \cup \emptyset = a$$

$$a \cup a = a$$

$$a \cup b = b \cup a$$

$$a \cup (b \cup c) = (a \cup b) \cup c$$

You should spend a few moments convincing yourself of the truth of these statements. You may also try to write out formal proofs.

There are corresponding facts about intersections:

Theorem 4 *For any sets a, b, c,*

$$a \cap \emptyset = \emptyset$$

$$a \cap a = a$$

$$a \cap b = b \cap a$$

$$a \cap (b \cap c) = (a \cap b) \cap c$$

There are two important relations which involve both unions and intersections. These are called the <u>DISTRIBUTIVE LAWS</u> and are definitely not as simple as the facts observed above.

Theorem 5 *For any sets a, b, c*

$$a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$$

and

$$a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$$

We shall not prove these but in some of the examples below you will check that the distributive laws do hold.

HOMEWORK

1. Let
$$a = \{1, 2, 3, 4\}, \qquad b = \{2, 3, 4, 8\}, \qquad c = \{3, 1, 7, 5\}$$
Determine:

   (i) $a \cup b$

   (ii) $a \cap b$

   (iii) $b \cup c$

   (iv) $b \cap c$

   (v) $a \cup c$

   (vi) $a \cap c$

   (vii) $a \cup (b \cap c)$

   (viii) $(a \cup b) \cap (a \cup c)$

   (ix) $a \cap (b \cup c)$

(x) $(a \cap b) \cup (a \cap c)$

(xi) Check that the distributive laws hold for these particular sets a, b, c.

2. For any set a, denote by a^* the set $a \cup \{a\}$:

$$a^* = a \cup \{a\}$$

The set a^* is called the <u>successor</u> of a, and is also denoted $a + 1$.

(i) Show that $\emptyset^*$ is 1.

(ii) Show that $1^* = 2$

(iii) Determine 2^* and 3^*

1.8 Boolean Algebra

Very often one works with a set $\mathcal{U}$ and focuses only on elements of this set. This set is called the <u>universal set</u> for the given context.

For example, in some context, one may only wish to discuss rational numbers; in this situation the set $\mathcal{U}$ is $\mathbf{Q}$, the set of all rational numbers.

So suppose we have a universal set $\mathcal{U}$ in a given context. If $a \subset \mathcal{U}$ then the <u>complement</u> of a is the set of all elements of $\mathcal{U}$ which are not in a. The complement of a is denoted a^c. Thus

$$a^c = \{x | x \in \mathcal{U}, x \notin a\} \tag{1.6}$$

Read this as: a^c is the set of all objects x which are elements of $\mathcal{U}$ but not of a.

Lets look at an example. Say our universal set happens to be $\mathcal{U} = \{0, 1, 2, 3\}$. Then the complement of $\{0, 1\}$ is $\{2, 3\}$:

$$\{0, 1\}^c = \{2, 3\}$$

The complement of $\{1, 3, 0\}$ is $\{2\}$:

$$\{1, 3, 0\}^c = \{2\}$$

The complement of $\{0\}$ is $\{1, 2, 3\}$. Now the empty set $\emptyset$ is also a subset of $\mathcal{U}$. What is its complement? Well, *all* elements of $\mathcal{U}$ are in the complement of $\emptyset$, and so

$$\emptyset^c = \mathcal{U}$$

Check for yourself that:

$$\mathcal{U}^c = \emptyset$$

Thus for every universal set $\mathcal{U}$:

$$\emptyset^c = \mathcal{U} \qquad \text{and} \qquad \mathcal{U}^c = \emptyset$$

We state the next few observations formally as a Proposition:

Proposition 1 *For every $a \subset \mathcal{U}$,*

$$(a^c)^c = a \tag{1.7}$$

Also,

$$a \cup a^c = \mathcal{U} \qquad \textit{and} \qquad a \cap a^c = \emptyset \tag{1.8}$$

You should prove these for yourself.

Less easy to see are the following relations involving unions, intersections, and complements.

Theorem 6 *For any sets $a, b \subset \mathcal{U}$,*

$$(a \cup b)^c = a^c \cap b^c$$

and

$$(a \cap b)^c = a^c \cup b^c$$

Here is a formal proof of the first equality.

Proof. We will only prove the first equality. The proof consists of two steps. First we show that every element of $(a \cup b)^c$ is in $a^c \cap b^c$. In the second step we show that every element of $a^c \cap b^c$ is in $(a \cup b)^c$. Together, this will show that the sets $a^c \cap b^c$ and $(a \cup b)^c$ have exactly the same elements, i.e. these sets are equal.

If x is any element of $(a \cup b)^c$ then x is outside $a \cup b$, and so x is neither in a nor in b. Thus such an x is in both a^c and in b^c, i.e. in $a^c \cap b^c$. This shows that every element of $(a \cup b)^c$ is in $a^c \cap b^c$.

Now consider any element x in $a^c \cap b^c$. This x is in both a^c and b^c. This means that x is neither in a nor in b. Therefore, x can't be in $a \cup b$. So $x \in (a \cup b)^c$.

Thus we have shown that $a^c \cap b^c$ and $(a \cup b)^c$ have exactly the same elements, and so these sets are equal. ♣

Recall that $\mathcal{P}(\mathcal{U})$, the power set of $\mathcal{U}$, is the set of all subsets of $\mathcal{U}$. There are three basic things one can do with the elements of $\mathcal{U}$: unions, intersections, and complements:

$$a \cup b \qquad a \cap b \qquad a^c$$

Here is the complete list of all the fundamental facts about these operations: for any $x, y, z \in \mathcal{U}$:

$$x \cup \emptyset = x, \qquad x \cup \mathcal{U} = \mathcal{U}$$

$$x \cup x = x$$

$$x \cup y = y \cup x \qquad \text{: commutativity of } \cup$$

$$x \cup (y \cup z) = (x \cup y) \cup z \qquad \text{: associativity of } \cup$$

$$x \cap \emptyset = \emptyset, \qquad x \cap \mathcal{U} = x$$

$$x \cap x = x$$

$$x \cap y = y \cap x \qquad \text{: commutativity of } \cap$$

$$x \cap (y \cap z) = (x \cap y) \cap z, \qquad \text{: associativity of } \cap$$

$$x \cup (y \cap z) = (x \cup y) \cap (x \cup z), \qquad x \cap (y \cup z) = (x \cap y) \cup (x \cap z) \qquad \text{: distributive laws}$$

$$\emptyset^c = \mathcal{U} \qquad \mathcal{U}^c = \emptyset$$

$$(x^c)^c = x$$

$$(x \cup y)^c = x^c \cap y^c \qquad (x \cap y)^c = x^c \cup y^c \qquad \text{: de Morgan's laws}$$

One says that $\mathcal{U}$ is a <u>Boolean algebra</u> with the operations $\cup$,$\cap$, and complementation $x \mapsto x^c$.

HOMEWORK

1. Let $\mathcal{U} = \{0, 1, 2, 3, 4, 5\}$. Consider the sets $x = \{1, 2, 3\}$, $y = \{1, 3, 5\}$, and $z = \{2, 3, 4\}$. Determine x^c, y^c, and z^c. Verify that each of the Boolean algebra properties hold for the sets x, y, z.

1.9 PARADOXES

Suppose we consider the set of *all* sets. Lets call this gigantic set G. So G is the set of all sets. Thus *every* set is an element of G. Now G itself is a set. So G must be an element of G! Thus this gigantice set G satisfies the somehow disturbing property

$$G \in G$$

Even though this is unsettling there is no obvious reason why this should be impossible. However, as we shall soon see we will run into a paradoxical situation when we focus on a certain special subset of G. This subset, lets call it P for "paradoxical", will be defined in a twisted way: we take P to be *the set of all sets x which are not elements of themselves.* Thus

$$P = \{\text{all } x \text{ such that } x \notin x\}$$

At first there seems nothing wrong with this. However, here is the big question:

Is P an element of itself?

As we try to answer this we see we are in deep trouble. If P were indeed an element of itself, i.e. if $P \in P$, then the definition of P shows that P would not be an element of P, i.e. $P \notin P$. On the other hand, if P were not an element of itself, i.e. if $P \notin P$, then the definition of P shows that P would indeed be an element of P. Thus we are boxed into a paradox with no escape.

When mathematicians first ran into such paradoxes it was decided that certain rules of order must be imposed on set theory. In order to have a framework free of paradoxes we must give up some freedoms: only certain types of sets should be "allowed" to exist. So certain rules, called the <u>axioms</u> of set theory, are chosen which specify strict rules according to which sets may be constructed. We shall not pursue this further but let us note a few points. First of all the giant set G as well as the paradoxical set P are not sets which can be constructed within the allowed rules.

The axioms of set theory assert first of all that the empty set $\emptyset$ is an allowed set. In fact, this is practically the single brick with which the entire edifice of mathematics is constructed within set theory. Then the axioms provide certain strict rules which may be used to construct new sets from known ones. For example, from $\emptyset$ we allowed to construct the set $1 = \{\emptyset\}$,

and then we are allowed to construct $2 = \{\emptyset, 1\}$, and so on. The axioms also declare that the infinite set $\omega_0 = \{0, 1, 2, ...\}$ is allowed.

Further discussion of these matters would lead us into deeper aspects of set theory. So we stop and turn to more practical matters.

Chapter 2

Mappings

Within mathematics, all sets are sets of mathematical objects. However, for applications, as well as for illustration of ideas, we shall often discuss sets whose elements are not necessarily mathematical objects. For example, we may consider the set of all students in a class, or the set of all people who live in a city, or the set of months in a year, etc.

Consider sets A and B. A mapping from A to B is, conceptually, a rule that associates an element of B to each element of A.

For example, suppose A is the set of students in a class, and $B = \{\text{January, February,..., December}\}$ is the set of months in the year. Consider now a table which lists the birth-month against each student in the class. This associates to each element of A (i.e. each student in the class) an element of B (the month in which the student was born). This is an example of a mapping from A to B. Note two things: (i) to each element of A is associated an element of B, (ii) no element of A is associated to more than one element of B.

We will see how the notion of a mapping can be given a precise definition within set theory.

2.1 Ordered Pairs

Consider objects x and y. There is a special set we can construct from x and y which turns out to be extremely useful. It is the set

$$\{\{x\}, \{x, y\}\}$$

This set is called an ordered pair and is denoted (x, y). Thus

$$(x, y) = \{\{x\}, \{x, y\}\} \tag{2.1}$$

It is very important to note :

- (x, y) is NOT the same as $\{x, y\}$. Do not be sloppy with brackets!

At this stage it is not at all why (x, y) is useful. But its value will become clear slowly.

Exercise. Show that $(2, 3) \neq (3, 2)$. [Thus the *order* in which the elements 2 and 3 appear is important.]

Solution. We write out $(2, 3)$ and $(3, 2)$ in full:

$$(2, 3) = \{\{2\}, \{2, 3\}\} \qquad (3, 2) = \{\{3\}, \{3, 2\}\}$$

Clearly these two sets do not have exactly the same elements; for instance, $\{2\}$ is an element of $(2, 3)$ but not of $(3, 2)$. So $(2, 3)$ is not equal to $(3, 2)$.

Exercise. Suppose $(a, b) = (1, 5)$. Show that a must be 1 and b must be 5.

Solution. Writing out $(a, b) = (1, 5)$ in full we have

$$\{\{a\}, \{a, b\}\} = \{\{1\}, \{1, 5\}\}$$

So, since two sets are equal only when they have exactly the same elements, we see that

(i) EITHER $\{a\} = \{1\}$ and $\{a, b\} = \{1, 5\}$,

(ii) OR $\{a\} = \{1, 5\}$ and $\{a, b\} = \{1\}$.

Now (ii) is not possible because $\{a\}$ contains just one element a while $\{1, 5\}$ contains two elements (since 1 and 5 are two distinct elements). Thus the only possibility is (i). Thus

$$\{a\} = \{1\} \qquad \text{and} \qquad \{a, b\} = \{1, 5\}$$

The first equality tells us that $a = 1$. And then the second equality tells us that b must be equal to 5. Thus

$$a = 1 \qquad b = 5$$

as claimed. ♣

The above exercises illustrate crucial properties of an ordered pair.

2.2 Cartesian Product of Sets

Consider sets A and B.

$$A = \{1, 3, 5\} \qquad \text{and} \qquad B = \{3, 2, 4\}$$

The cartesian product $A \times B$ is the set of all ordered pairs (a, b) which can be formed by choosing a from A and b from B:

$$A \times B = \{(a, b) \mid a \in A,\, b \in B\}$$

For example, if

$$A = \{1, 3, 5\} \qquad \text{and} \qquad B = \{3, 2, 4\}$$

then

$$A \times B = \{(1,3), (1,2), (1,4), (3,3), (3,2), (3,4), (5,3), (5,2), (5,4)\}$$

In contrast,

$$B \times A = \{(3,1), (3,3), (3,5), (2,1), (2,3), (2,5), (4,1), (4,3), (4,5)\}$$

Note also that

$$A \times A = \{(1,1), (1,3), (1,5), (3,1), (3,3), (3,5), (5,1), (5,3), (5,5)\}$$

For any set y,

$$\emptyset \times y = \emptyset \qquad \text{and} \qquad y \times \emptyset = \emptyset$$

because there is simply no ordered pair whose first/second element belongs to $\emptyset$.

HOMEWORK

1. Let $P = \{0, 1, 2\}$, $Q = \{5, 1, 3\}$, $R = \{1, 2\}$, $S = \{1\}$, $T = \{2\}$. Write out the sets

$$P \times Q =$$
$$Q \times P =$$

$$(P \times Q) \cap (Q \times P) =$$

$$R \times R =$$

$$R \times (R \times R) =$$

$$(R \times R) \times R =$$

$$S \times Q =$$

$$T \times Q =$$

$$(S \times Q) \cap (T \times Q) =$$

2.3 Relations

Consider sets A and B. We have seen that $A \times B$ is the set of *all* ordered pairs (a, b) with a drawn from A and b from B. We will generally be concerned with smaller sets of ordered pairs with first element drawn from A and the second from B. Such a set $\mathcal{R} \subset A \times B$ is called a <u>relation</u> from A to be B. If a particular ordered pair (x, y) belongs to $\mathcal{R}$ then we say that x is related to y by $\mathcal{R}$.

Example. Let $F = \{$alice, betty, carla$\}$ and $M = \{$al, bob, charles$\}$. The set

$$f = \{(\text{alice,bob}), (\text{betty, charles}), (\text{alice,al}), (\text{carla, al})\}$$

is a relation from F to M.

Often we are concerned with relations from a set to itself. If A is a set then a relation on A is just a subset of $A \times A$. There are several types of relations that appear in mathematics:

1. a relation is <u>reflexive</u> if each element is related to itself

2. a relation is <u>symmetric</u> if whenever x is related to y then y is also related to x

3. a relation is <u>transitive</u> if whenever x is related to y and y is related to z then x is related to z.

Exercise. Consider the set $\mathbf{Z} = \{0, 1, -1, 2, -2, 3, -3, ...\}$ of all integers. Let E denoted the subset consisting of *even* integers: $E = \{0, 2, -2, 4, -4, ...\}$. Let B be the set of all ordered pairs (m, n) where m and n are integers such that $m - n \in E$. Thus B is a relation on $\mathbf{Z}$. For example, $(3, 7) \in E$ because 3 and 7 are integers and $3 - 7 = -4$ which is in E. Also, $(7, 7)$ is in B because 7 is an integer and $7 - 7 = 0$ which is in E. On the other hand, $(2, 5)$ is not in B because $2 - 5 = -3$ is not in E.

(a) Is $(3, 5) \in B$? Is $(-2, 4) \in B$?

(b) Is the relation B reflexive?

(c) Is the relation B symmetric?

(d) Is the relation B transitive?

2.4 Mapping

A <u>mapping</u>, or a <u>map</u>, from a set A to a set B is a relation from A to B such that each element of A is related to exactly one element of B. In more detail, a mapping f from A to B is a set of ordered pairs (a, b) with $a \in A$ and $b \in B$ such that for each element $x \in A$ there is exactly one element $y \in B$ such that $(x, y) \in f$.

Example. Let $T = \{a, b, c\}$ (where a, b, c are distinct objects) and $V = \{1, 3\}$. Let

$$f = \{(a, 3), (b, 1), (c, 3)\}$$

Then f is a mapping from T to V (we give it the name f only for ease of reference). So is also the set

$$g = \{(a, 1), (b, 1), (c, 1)\}$$

Next let

$$h = \{(a, 1), (b, 1), (c, 3), (a, 3)\}$$

$$k = \{(a, 1), (c, 3)\}$$

Neither h nor k is a mapping from T to V. The reason h is not a mapping is that a is related to both 1 and 3. The reason k is not a mapping is that b is not related to any element in V. ♣

If f is a mapping from D to C we express this by writing

$$f : D \to C$$

which one reads: f is a mapping from D to C. In this situation, the set D is called the <u>domain</u> of the mapping f, and C is called the <u>codomain</u> for f. If f relates an element $x \in D$ to an element $y \in C$, i.e. if $(x, y) \in f$ then we express this by writing $f(x)$ for y:

$$y = f(x) \quad \textit{means exactly that } (x, y) \in f$$

In this case we say that y is the *image of* x *under* f. This means exactly that (x, y) is an element of f.

Example. Let $S = \{1, 2, 3\}$ and $D = \{p, q\}$, and let $h : S \to D$ be the mapping

$$h = \{(1, p), (2, p), (3, q)\}$$

Then

$$h(1) = p \qquad \text{in words: } p \text{ is the image of 1 under } h$$

$$h(2) = p \qquad \text{in words: } p \text{ is the image of 2 under } h$$

and

$$h(3) = q \qquad \text{in words: } q \text{ is the image of 1 under } h$$

In contrast, in this example, $h(p)$ has no meaning because p is not an element of the domain of h. ♣

For a mapping $f : A \to B$, the <u>image</u> of f is the set of all elements of B which are images of elements in A under f.

For example, if $A = \{3, 4, 5\}$ and $B = \{c, x, 7\}$, and $g = \{(3, 7), (4, c), (5, 7)\}$, then the image of g is $\{7, c\}$.

<u>Notation</u>.The set of all mappings $A \to B$ is denoted B^A.

For example, if $T = \{a, b\}$ and $S = \{3, 4\}$ then S^T is the set whose elements are the mappings

$$\{(a, 3), (b, 3)\}, \qquad \{(a, 3), (b, 4)\}, \qquad \{(a, 4), (b, 3)\}, \qquad \{(a, 4), (b, 4)\}.$$

Thus, writing it out in full as a set,

$$S^T = \{\{(a, 3), (b, 3)\}, \{(a, 3), (b, 4)\}, \{(a, 4), (b, 3)\}, \{(a, 4), (b, 4)\}\}$$

Though a mapping is, technically, a set of ordered pairs, few people actually think of a mapping in this way. A common way to view a mapping

is to think of it as a "rule" that relates to each element of the domain an element of the codomain. There are other ways to think of a mapping. In some contexts, a mapping is specified by a "formula" (the mapping which related each real number to twice itself is specified by the formula $2x$) and some like to think of the formula as the mapping. Sometimes one draws a picture, perhaps a graph, to illustrate a mapping. One way a mapping often appears in applications is from a table with two columns (or rows) listing the objects which are related to each other. This is the closest to the technical definition of a mapping.

HOMEWORK

Problem 1 Let $C = \{1, 2, 3\}$ and $D = \{p, q\}$ (where p and q are two distinct objects). Here is the list of <u>all</u> the mappings $C \to D$:

$$\begin{array}{ccc} & \{(1,p),(2,p),(3,p)\} & \\ \{(1,p),(2,p),(3,q)\} & \{(1,p),(2,q),(3,p)\} & \{(1,q),(2,p),(3,p)\} \\ \{(1,q),(2,q),(3,p)\} & \{(1,q),(2,p),(3,q)\} & \{(1,p),(2,q),(3,q)\} \\ & \{(1,q),(2,q),(3,q)\} & \end{array}$$

Now write out <u>all</u> mappings $D \to C$ (there are nine such maps), and then all mappings $D \to D$ (there are four such maps).

Problem 2 With D as in Problem 1, write out the set D^D.

Before doing Problem 3, recall that a set h is a mapping from a set P to a set Q if :(i) h is a subset of $P \times Q$, and (ii) for each element p of P there is exactly one element q in Q such that (p, q) belongs to h. It is also useful to understand this in a 'negative' way: a set h is *not* a mapping from P to Q if and only if either

(a) h is not a subset of $P \times Q$,

or (b) there exists an element $p \in P$ such that for no $q \in Q$ is (p, q) is an element of h,

or (c) there exists an element $p \in P$ such that there is more than one $q \in Q$ for which (p, q) is an element of h.

If a set h fails to satisfy (a), (b), (c) then it must be a mapping $P \to Q$.

Problem 3. Convince yourself of the following points. Let A be any set. Then $\emptyset$ is a mapping $\emptyset \to A$. This is in fact the only mapping $\emptyset \to A$. However, there is no mapping at all $A \to \emptyset$, unless A itself is empty.

2.5 Injective, Surjective, Bijective Maps

A map $f : A \to B$ is said to be injective if different elements of A have different images, i.e. if no two different elements of A have the same image.

For example, suppose $A = \{1, 2, 3\}$ and $B = \{3, 4, 5, 6\}$ and

$$f = \{(1, 3), (2, 5), (3, 6)\} \qquad \text{and} \qquad g = \{(1, 5), (2, 3), (3, 5)\}$$

Then f and g are both maps $A \to B$, f is injective but g is not injective. The reason g is not injective is that $g(1)$ and $g(3)$ both equal 5.

A mapping $f : C \to D$ is surjective if every element of D is in the image of f.

For example, suppose $T = \{1, 2, 3, 4\}$ and $S = \{2, 3, 5\}$, and

$$f = \{(1, 2), (2, 3), (3, 3), (4, 5)\} \qquad h = \{(1, 2), (2, 3), (3, 3), (4, 2)\}$$

Then f and g are both maps $T \to S$, f is surjective but h is not surjective. The reason h is not surjective is that the element $5 \in S$ is not in the image of h.

A mapping $f : A \to B$ which is both injective and surjective is called a bijection. A little thought or experimentation shows that if you take two finite sets A and B, a bijection $A \to B$ exists if and only if A and B have the same number of elements.

HOMEWORK

1. Let $S = \{a, b, c\}$ (where a, b, c are distinct), and $T = \{4, 5\}$. Write down all maps $S \to T$, all maps $T \to S$, and all maps $T \to T$. Write against each map if it is injective/surjective/bijective.

2. Let $A = \{p, q, r, s\}$ (where p, q, r, s are distinct), and $B = \{1, 3\}$. Write down all maps $A \to B$, all maps $B \to A$, and all maps $B \to B$ (and, if you have the patience, all maps $A \to A$!). Write against each map if it is injective/surjective/bijective.

3. Consider any set with three elements, say $S = \{a, b, c\}$. Produce a bijection $3 \mapsto S$ (Recall that $3 = \{0, 1, 2\}$). Is it possible for there to be a bijection of any other number onto S?

4. Consider a set with four elements, say $V = \{p, q, r, s\}$. Produce a bijection $4 \mapsto V$. Is it possible for there to be a bijection of any other number onto V?

2.6 Counting/Cardinality

Recall first how we defined the numbers formally: 0 is the empty set $\emptyset$, 1 is the set $\{0\}$, 2 is the set $\{0, 1\}$, 3 is the set $\{0, 1, 2\}$, and so on.

When we want to determine the number of elements in a set we count them off one by one until we have covered all the elements. For example, the set $\{a, b, c, d, e, f\}$ has six elements. This allows us to set up a bijection $6 \mapsto \{a, b, c, d, e, f\}$ as follows (recall that 6 is the set $\{0, 1, 2, 3, 4, 5\}$):

$$\{(0, a), (1, b), (2, c), (3, d), (4, e), (5, f)\}$$

More generally, if there is a bijection from a number N (say 15, for instance) onto a set S then the set S has exactly N elements, and we write this symbolically as

$$\#S = N$$

Technically, this is short hand for the statment: there is a bijection $N \to S$. But you read this as: S has N elements.

For example, $\#U = 8$ means that the set U has eight elements.

A set for which is not in bijection with any of the numbers $0, 1, 2, 3, 4, ...$ is said to be <u>infinite</u>.

There is a theory, called the theory of <u>cardinal numbers</u>, invented by Georg Cantor which is used to properly extend the concept of "number of elements" to infinite sets. It is to study infinite sets and their cardinality that Cantor invented the whole structure of set theory!

HOMEWORK

1. Let $A = \{a, b\}$ and $B = \{x, y, z\}$. Find $\#(A^B)$.

2.7 Sequences

Recall that A^B denotes the set of all mappings $B \to A$.

Consider now any non-empty set A and let us see what an element of A^3 looks. Recall that $3 = \{0, 1, 2\}$. Thus an element of A^3 is a mapping $3 \to A$, i.e. a mapping $\{0, 1, 2\} \to A$. Suppose, for example, $A = \{a, b, c, d, e, f\}$. Then A^3 contains, for instance, the element

$$\{(0, b), (1, a), (2, e)\}$$

It is conventional to write this element simply as

$$(b, a, e)$$

That is,

$$(b, a, e) \text{ is a short way of writing the map } \{(0, b), (1, a), (2, e)\}$$

Similarly, (a, f, b) is the map $\{(0, a), (1, f), (2, b)\}$.

So, with this notation, A^3 is the set of all triples (x_1, x_2, x_3), where x_1, x_2 and x_3 are elements of A.

Similarly, elements of A^4 are written in the form (x_1, x_2, x_3, x_4). Thus, with $A = \{a, b, c, d, e, f\}$, an example of an element of A^4 is (b, c, b, e).

Recall the set

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

In many situations it is necessary to consider maps $\mathbf{N} \to A$, where A is some set. If s is such a mapping then it has the form

$$s = \{(1, s_1), (2, s_2), (3, s_3), ...\}$$

where $s_1, s_2, s_3, ...$ are elements of A. As a matter of convention, one writes s simply as $(s_1, s_2, s_3, ...)$.

An example of a sequence of integers is

$$(3, -2, 1, -5, 11, 0, -8, 9, ...)$$

This is really a short form for the mapping

$$\{(1, 3), (2, -2), (3, 1), (4, -5), (5, 11), (6, 0), (7, -8), (8, 9), ...\}$$

A mapping $\mathbf{N} \to A$ is called a <u>sequence</u> of elements of A.

The set of all sequences in A is thus the set $A^{\mathbf{N}}$.

2.8 Composition of Mappings

Consider a mapping $f : A \to B$ and a mapping $g : B \to C$. There is a simple way to put these together to obtain a mapping $A \to C$. This new mapping is called the composite of f with g and is denoted $g \circ f$. It is specified by the formula

$$(g \circ f)(x) = g(f(x)) \qquad \text{for all } x \in A$$

In words, $g \circ f$ associates to each $x \in A$ the element $g(f(x)) \in C$.

The best way, as usual, to understand this notion is by looking at an example. So let $S = \{1, 2, 3\}$, $T = \{3, 4, 5\}$, and $V = \{7, 8\}$, and let $p : S \to T$ and $w : T \to V$ be the maps given by

$$p = \{(1, 4), (2, 3), (3, 4)\} \qquad w = \{(3, 8), (4, 7), (5, 8)\}$$

Then $w \circ p : S \to V$ is given by

$$w \circ p = \{(1, 7), (2, 8), (3, 7)\}$$

Here is explanation in more detail of how we found this. To write out $w \circ p$ in full, we need to know what the images of 1, 2, and 3 are, respectively, under $w \circ p$. The image of 1 under $w \circ p$ is, by definition, $w(p(1))$. Since $p(1)$ is 4, we see that the image of 1 under $w \circ p$ is $w(4)$. But then, $w(4)$ is 7. Thus, $w \circ p$ pairs 1 with 7. This gives us the first entry $(1, 7)$ in $w \circ p$. One finds the other entries similarly. With just a little practice this becomes very easy and you should be able to figure out the composite with just a glance at w and p.

HOMEWORK

Let $A = \{5, 6, 7\}$. Let I, f, and g, be the maps $A \to A$ given by

$$I = \{(5, 5), (6, 6), (7, 7)\}$$

$$f = \{(5, 7), (6, 5), (7, 6)\}$$

$$g = \{(7, 5), (5, 6), (6, 7)\}$$

Work out the composites $I \circ f$, $f \circ I$, $I \circ I$, $I \circ g$, $g \circ I$, $f \circ g$, $g \circ I$, $f \circ f$, and $g \circ g$.

2.9 Permutations

Recall that a mapping $f : A \to B$ is bijective if it is both injective and surjective. In this case we also say that f maps A one-to-one onto B, or that it sets up a one-to-one correspondence between A and B.

Often we are interested in bijective maps from a set onto itself. A bijective mapping $A \to A$ is called a permutation on A.

For example, let $S = \{1, 2\}$. Then the following maps $S \to S$ are permutations on S:

$$\{(1,1),(2,2)\} \qquad \{(1,2),(2,1)\}$$

If you write out all the maps $S \to S$ you will see that the only permutations on S are the two maps listed above.

HOMEWORK

> Let $T = \{a, b, c\}$, were a, b, c are three distinct objects. Write out all the maps $T \to T$. Mark which are injective/surjective/bijective. List all the permutations on T.

2.10 Infinite sets

We have noted before that if A and B are finite sets then a bijection $A \to B$ exists if and only if A and B have the same number of elements. For infinite sets the situation is more complex because we have not yet set up a notion of what it means for two sets to have the same number of elements if both are infinite sets.

Consider the set

$$\omega_0 = \{0, 1, 2, 3, 4, 5, 6, ...\}$$

and the set E of all even numbers among these,

$$E = \{0, 2, 4, 6, 8, ...\}$$

Clearly

$$E \subset \omega_0$$

So it may seem right to say that ω_0 contains a greater number of elements than E. However, there is a simple bijection $\omega_0 \to E$! Here it is:

$$\{(0,0),(1,2),(2,4),(3,6),(4,8),(5,10),...\}$$

This map pairs each element of ω_0 with its double: $x \mapsto 2x$.

Thus for infinite sets A and B it is possible for a bijection $A \to B$ to exist even if B is "smaller" than A in the sense that $B \subset A$ and $B \neq A$.

Two sets A and B are said to have the same cardinality if there is a bijection from one to the other. In the case of finite sets, this is the same as saying that they have the same number of elements.

Chapter 3

Some Counting Formulas

In this chapter we shall learn how to determine the cardinalities of some sets.

Given finite sets A, B, C, we will see how to determine the number of elements in $A \cup B$, in $A \cup B \cup C$, $A \times B$, in A^B, and we will also learn how to count the number of injective mappings $B \to A$.

In this chapter, $|A|$ will denote the number of elements in a set A. For example,

$$|\emptyset| = 0, \qquad \text{and} \quad |\{a, b, c\}| = 3,$$

assuming that a, b, c are distinct.

3.1 Counting elements in unions

Consider the sets

$$F = \{p, q, r, t\} \qquad \text{and} \qquad G = \{q, r, s, t, u\}$$

So $|F| = 4$ and $|G| = 5$. It might seem at first that $|F \cup G|$ is $4 + 5 = 9$, but

$$F \cup G = \{p, q, r, s, t, u\}$$

has 6 elements. The reason for this is that F and G have 3 elements (q, r, and t) in common, and so simply adding 4 and 5 counts these three elements twice. So $4 + 5$ is three more than the correct value for $|F \cup G|$; thus $|F \cup G|$ should really by $4 + 5 - 3$, which is indeed the correct value 6.

Generalizing this observation we obtain the formula

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

for any finite sets A and B.

The way to understand this formula is by realizing that in doing the sum $|A|+|B|$ one counts the elements in common, i.e. those in $A \cap B$ twice (once when counting A and again when counting B), and so the correct value of $|A \cup B|$ is obtained by subtracting $|A \cap B|$ from $|A| + |B|$.

There is a more involved but similar formula for three sets. For finite sets A, B, and C,

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

The reasoning for this is just as before. In the sum $|A| + |B| + |C|$ an element which lies in $B \cap C$, but not in A, is counted twice and so we can try to correct for the overcounting by subtracting $|B \cap C|$. Similarly, we subtract $|C \cap A|$ and $|A \cap B|$. But now each element of $A \cap B \cap C$ has been counted three times in $|A|+|B|+|C|$ but subtracted off three times in doing $-|B \cap C| - |C \cap A| - |A \cap B|$. Thus the elements of $A \cap B \cap C$ have been left out all together, and so we add $|A \cap B \cap C|$ to get the correct answer.

Example. In a town of 100 people, 50 subscribe to magazine A and 30 to magazine B. Forty people subscribe to neither magazine. How many subscribe to both?

Solution: Let A denote the set of people who subscribe to magazine A, and B the set of people who subscribe to magazine B. Since we are given that forty of the hundred people subscribe to neither magazine, $A \cup B$ must have 60 elements. We are also given that $|A| = 50$ and $|B| = 30$. We have to find $|A \cap B|$, the number of people who subscribe to both magazines. From the formula

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

we then have

$$60 = 50 + 30 - |A \cap B|$$

So

$$|A \cap B| = 20,$$

i.e. 20 people subscribe to both magazines.

Now try the following problem:

Exercise. In a group of fifty students, thirty are taking Math 1100 and forty are taking English 1234. Five students are taking neither of these courses. Determine how many are taking both the courses.

3.2 Counting elements in $A \times B$

Consider now finite sets A and B. The cartesian product $A \times B$ is the set of all ordered pairs with first element drawn from A and the second element drawn from B. Suppose for instance $|A| = 3$ and $|B| = 2$, say $A = \{a_1, a_2, a_3\}$ and $B = \{b_1, b_2\}$. Then

$$A \times B = \{(a_1, b_1), (a_1, b_2),\ (a_2, b_1), (a_2, b_2),\ (a_3, b_1), (a_3, b_2),\ \}$$

This has $3 \times 2 = 6$ elements. We can see why this is 3×2: each of the three elements of A is paired with each of the two elements of B, producing a total of $2 + 2 + 2$, i.e. 3×2 possible pairs.

More generally,

$$|A \times B| = (|A|)(|B|)$$

The $\times$ on the left side is the cartesian product of sets, while the right side is the product of the numbers $|A|$ and $|B|$.

HOMEWORK.

1. Let $P = \{a, b, c\}$ and $Q = \{b, c, e, f\}$, where a, b, c, e, f are all distinct objects. Work out $P \times Q$ and verify that $|P \times Q|$ is indeed equal to $|P|\,|Q|$.

3.3 Counting elements in A^B

Consider a set X with four elements, and a set Y with three elements. Say, for instance, $X = \{a, b, c, d\}$ and $Y = \{p, q, r\}$. We wish to find out how many mappings $X \to Y$ there are.

Now to form a mapping $f : X \to Y$, we must specify an image for each element of X. For the element a in X, we have 3 possible elements in Y we can pair it with: we could do either (a, p), or (a, q), or (a, r). Having picked a choice for partner for a, we then look at b and see that b also has, of course, 3 possible partners from Y. Thus, just between a and b we have 3×3 possible pairings with elements of Y. Proceeding to c, we again have 3 choices. So, with a, b, c we have a total of $3 \times 3 \times 3$ possible pairings with Y. Finally, including d, we have $3 \times 3 \times 3 \times 3$ possible ways to form a mapping $X \to Y$. Thus, we conclude that Y^X has 3^4 elements. We observe that

$$|Y^X| = |Y|^{|X|}$$

The reasoning we used is clearly valid even if X and Y had other numbers of elements. So we obtain the general formula

$$|A^B| = |A|^{|B|}$$

HOMEWORK

1. Let $X = \{a, b, c\}$.

   a. Write out $\mathcal{P}(X)$, the set of all subsets of X.

   b. Write out $\{0, 1\}^X$, the set of all mappings $X \to \{0, 1\}$.

   c. Determine $|\mathcal{P}(X)|$.

   d. Determine $|\{0, 1\}^X|$.

   e. Try to find a natural bijection from $\mathcal{P}(X)$ onto $\{0, 1\}^X$.

3.4 Counting injective mappings

Consider a set X with 5 elements and a set Y with 3 elements. Say, for instance, $X = \{a, b, c, d, e\}$ and $Y = \{p, q, r\}$. We wish to determine how many injective mappings there are $Y \to X$.

For an injective mapping $Y \to X$ we must specify a partner in X for each element of Y in such a way that different elements of Y have different partners.

For the element $p \in Y$ we have 5 possible partners from X (i.e. we could take any of the pairings (p, a), (p, b), (p, c), (p, d), and (p, e)).

Having chosen a partner for p, when we turn to $q \in Y$, we see that q has only 4 choices left, because q is not allowed to be paired with the element already selected for p.

Note that for each choice made by p, q has 4 choices. Since p itself has 5 choices, we conclude that between p and q, there are 5×4 possible pairings with elements of X so that p and q get paired with different elements.

Next, *having chosen partners for* p and q, we only have 3 possible choices left in X to pick from. Thus for each choice made by p and q there are 3 choices that r has. Snce p and q together had a total of 5×4 choices, we see that p, q, r all together have $5 \times 4 \times 3$ choices. Thus:

the total number of injective mappings $Y \to X$ is $5 \times 4 \times 3$, i.e. 60.

HOMEWORK

1. Let $A = \{1, 2, 3\}$ and $B = \{1, 2, 3, 4, 5, 6\}$. Show that there are 120 injective mappings $A \to B$. *Explain your reasoning completely.*

2. Consider a set A with 9 elements and a set B with 6 elements. How many mappings are $B \to A$ are there? How many of these mappings are injective?

3.5 Counting Permutations

Consider a set X with four elements. Say, $X = \{a, b, c, d\}$. Recall that a permutation on X is a bijective mapping $X \to X$. We wish to determine how many such mappings there are.

We now need an important observation about finite sets :

- *If X is a finite set then a mapping $X \to X$ which is injective is automatically surjective; and, conversely, a map $X \to X$ which is surjective is automatically injective.*

Thus for a map $X \to X$ to be bijective is equivalent to it being injective. Thus all we need to do is count the number of injective mappings $X \to X$. By the method of the preceding section we obtain the answer quickly:

$$4 \times 3 \times 2 \times 1$$

That is, there are 24 permutations of the four-element set X.

The product $4 \times 3 \times 2 \times 1$ is usually written in short as $4!$ (read: 4 factorial):

$$4! = 4 \times 3 \times 2 \times 1 = 24$$

The number of permutations on a five elements set is, similarly,

$$5! = 5 \times 4 \times 3 \times 2 \times 1 = 120$$

The only bijection $\emptyset \to \emptyset$ is $\emptyset$ itself; thus there is exactly one permutation on the zero-element set $\emptyset$. So

$$0! = 1$$

Easier to see is

$$1! = 1$$

Example. How many words (including all nonsense ones as well) can be formed be (re)arranging the letters of the word STOP?

Solution: Since the word has four letters, for the first letter we have 4 choices, then for the second letter we have 3 choices, for the third letter we have 2 choices, and finally for the last letter we have just 1 choice left. Thus there are a total of $4 \times 3 \times 2 \times 1 = 24$ such words which can be formed. The same argument can be viewed as counting the number of bijections $\{S, T, O, P\} \to \{S, T, O, P\}$, with the image of S being the letter which replaces S in STOP, the image of T the letter which replaces T, and so on.

HOMEWORK

1. Calculate the factorials o all numbers from 0 to 10.

2. How many words can be formed be arranging the letters of the word PAWS in all possible ways?

3.6 Combinations

Consider a set with five elements, say $X = \{a, b, c, d, e\}$. We want to find how many 2–element subsets X has. Of course, we could do this by listing all such subsets: $\{a, b\}$, $\{a, c\}$, $\{b, e\}$, ... But this is a long and exhausting method. Our goal is to come up with a more intelligent method.

Consider a map $f : \{1, 2\} \to X$. If f is injective then the image of this map, consisting of the elements $f(1)$ and $f(2)$ of X, is a two-element subset of X. Conversely, every two-element subset of X is the image of an injective mapping $\{1, 2\} \to X$.

For example, the subset $\{c, e\}$ is the image of the map $\{1, 2\} \to X$ given by $\{(1, c), (2, e)\}$. Observe that $\{c, e\}$ *is also the image of another map* $\{1, 2\} \to X$, given by $\{(1, e), (2, c)\}$.

The first attempt we can make to count the two-element subsets of X would be to simply count the number of injective mappings $\{1, 2\} \to \{a, b, c, d, e\}$. We know that there are $5 \times 4 = 20$ such mappings. However, as we have noticed above, each two-element subset of $\{a, b, c, d, e\}$ is the image of *two* injective mappings $\{1, 2\} \to X$. Thus the number of two-element subsets is actually half of 20, i.e. it is 10. In summary,

$$\text{the number of 2–element subsets of a 5–element set is } \tfrac{5\times 4}{2}$$

Now let us determine the number of three-element subsets of a seven-element set Y. We first note that each three-element subset is the image of an injective mapping $\{1,2,3\} \to Y$. There are $7 \times 6 \times 5 = 210$ such mappings. But many of these mappings have the same image, i.e. correspond to the same three-element subset. Indeed, given any particular injection $f : \{1,2,3\} \to Y$, we can permute $1,2,3$ to obtain obtain $3! = 6$ mappings mappings in all which have the same image. Thus among the 210 injections $\{1,2,3\} \to Y$, each map appears 6 times. So the actual number of three-element subsets of Y is $\frac{210}{6} = 35$. To summarize,

$$\text{number of 3–element subsets which a 7–element set has} = \frac{7\times6\times5}{3!}$$

Using the same strategy we see, for example, that the number of 5 element subsets of a 12–element set is

$$\frac{12 \times 11 \times 10 \times 9 \times 8}{5!}$$

This number is denoted $\binom{12}{5}$.

Similarly, $\binom{10}{6}$ denotes the number of six-element subsets which a ten-element set has, and is given by

$$\binom{10}{6} = \frac{10 \times 9 \times 8 \times 7 \times 6 \times 5}{6!}$$

HOMEWORK.

1. Consider a set X with 5 elements.

   a. How many 0–element subsets does X have?
   b. How many 1–element subsets does X have?
   c. How many 2–element subsets does X have?
   d. Determine the number of 3–element subsets of X.
   e. Determine the number of 4–element subsets of X.
   f. How many 5–element subsets does X have?
   g. How many subsets does X have in all.

   Summarize any observations you can make on the basis of the numbers you have calculated above.

3.7 More counting

Let us figure out the number of words which can be formed by arranging the letters of AIDA. If we use the method of the preceding section without examination we find the answer $4! = 24$. Here they are:

AIDA, ADIA, AIAD, ADAI, AAID, AADI,
IAAD, IADA, IDAA, IAAD, IADA, IDAA,
DIAA, DAIA, DAAI, DIAA, DAIA, DAAI,
AIDA, ADIA, AIAD, ADAI, AAID, AADI

A look at this list of 24 arrangements shows a problem: each word appears twice in the list. So actually there are only $12 = \frac{24}{2}$ distinct words.

Now we must understand *why* each word appears twice in the list. The reason is that for each word in the list, say AIDA, we can switch the two A's and obtain, instead of a new word, the same word again! This is why each word appears twice in the list.

The same argument works for the word CATALOG. The number of distinct words which can be formed by arranging the letters is

$$\frac{7!}{2} = \frac{7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1}{2} = 2520$$

Again, 7! would have been an overcount, and we divide by 2 to adjust for the presence of two A's.

Now suppose we try the same problem for the "word" AAABC. The naive count gives the answer $5! = 120$. However, each word in this list of 120 words is repeated several times. We have to figure out how many times each word appears in the list. For example, for the word BAACA every time we reorder the 3 A's we get back the same word BAACA. How many ways can we arrange the three A's in BAACA? The answer is, of course, 3!, i.e. 6. Thus each word in the list of 120 appears 6 times. So the total number of distinct words obtained by arranging the letters of AAABC is

$$\frac{120}{6} = 20$$

It is good to notice that the answer is

$$\frac{5!}{3!},$$

where 5 is the total number of letters in the word and 3 is the number of times A appears in the word.

If we try to same problem for the word $AAAABBBC$ we get first the naive overcount 8!. In adjusting for repeated letters we now have to adjust first for the 4 times A appears and then then 3 times B appears. So the correct answer is $\frac{8!}{4!3!}$.

HOMEWORK

1. Find the number of words which can be formed using exactly 5 A's, 3 B's, and 2 C's.