MATHEMATICS 300 — SPRING 2019

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

Part III

Contents

1 Sets **2**

1.1 What kind of thing is a set? 2

1.1.1 Sets with structure 6

1.1.2 How sets are different from other collective entities 7

1.1.3 Terms and sentences with variables: a review 7

1.1.4 Forming sets 10

1.1.5 The membership criterion 10

1.1.6 Forming sets of members of a given set 12

1.1.7 How to read the symbol "$\in$" 14

1.2 When are two sets equal? 15

1.2.1 Subsets 19

1.2.2 The empty set 22

1.2.3 The empty set is a subset of every set 23

1.2.4 Sets with one, two, three or four members 24

1.3 Operations on sets 27

1.4 The power set of a set 27

1.5 The union of two sets 28

1.6 The intersection of two sets 30

1.7 The difference of two sets 31

1.8 Complements 32

1.9 The symmetric difference of two sets 35

1.10 The Cartesian product of two sets 37

1.10.1 Ordered pairs 37

1.10.2 The Cartesian product of two sets 39

1.11 Important facts about the set operations 40

1.12 Some examples of proofs about sets 46

1.12.1 Proof of one of the distributive laws 46

1.12.2 Proofs of the De Morgan laws 48
1.12.3 A proof involving the symmetric difference 52

2 Relations and functions **55**
2.1 The definition of "relation" 55
2.1.1 How to think of a relation 55
2.1.2 Input, outputs, domain, range, source and target 56
2.2 Functions 58
2.2.1 An example of a function: the word "giraffe" 58
2.2.2 The precise mathematical definition of "function" 61
2.2.3 The definition of "value" of a function at a member of its domain 61
2.2.4 The definition of "set where a function takes values" 62
2.2.5 When are two functions equal? 62
2.2.6 The definition of "function mapping a set to a set" 63
2.2.7 The "input-to-output" way to write names of functions . . 63
2.3 Examples of functions 64
2.3.1 The integer part function 64
2.3.2 The "absolute value of a real number" function 65
2.3.3 Other "absolute value" functions 66
2.3.4 Squaring functions 67
2.3.5 Functions of two variables 69
2.3.6 Binary operations as functions 71
2.4 Composition of functions 74
2.4.1 The definition of "one-to-one function" 74
2.4.2 The composite of two one-to-one functions 75
2.4.3 The definition of "function onto a set" 75
2.4.4 The composite of two onto functions 76
2.5 The definition of "bijection" 76
2.5.1 The exchange lemma 78
2.5.2 The composite of two bijections 80
2.5.3 The identity function of a set 80
2.5.4 The inverse of a relation 81
2.5.5 The inverse of the inverse 83
2.5.6 The inverse of a bijection 83
2.5.7 Some problems 84

3 Finite sets **86**
3.1 An important notational convention: the sets $\mathbb{N}_k$ 86
3.2 Finite lists (a.k.a. finite sequences, or n-tuples) 86

3.2.1 The entries of a list: entries vs. members . . . 87
3.2.2 Describing sets and lists by enumeration . . . 89
3.2.3 Describing sets and lists using dummy variable notation . . 90
3.3 Finite sets . . . 91
3.3.1 What do we mean by "a list of all the members of A" . . . 91
3.3.2 Lists without repetitions and one-to-one functions . . . 92
3.3.3 Eliminating repetitions: an example . . . 93
3.3.4 Eliminating repetitions: a general theorem . . . 94
3.4 Finie sets and bijections . . . 95
3.5 Infinite sets . . . 95

4 Cardinality of sets **97**
4.1 Sets with the same cardinality . . . 97
4.2 Finite sets and their cardinality . . . 98
4.2.1 Can we talk about *the* cardinality of a finite set? The fundamental theorem of finite set cardinality theory . . . 99
4.2.2 Definition of "cardinality" of a finite set . . . 102
4.2.3 A trivial but important lemma . . . 103
4.2.4 Subsets of a finite set . . . 104
4.2.5 The Dirichlet pigeonhole principle . . . 105
4.2.6 Unions of finite sets . . . 107
4.2.7 Sets of subsets . . . 108
4.2.8 Cartesian products of finite sets . . . 108
4.3 Infinite sets . . . 108
4.3.1 Countable sets . . . 112
4.3.2 Do all infinite sets have the same cardinality? . . . 113
4.3.3 Consequences of Cantor's Theorem . . . 114
4.3.4 Comparing sizes of sets. The Cantor-Schroeder-Bernstein Theorem . . . 115
4.3.5 Infinitely many infinite cardinals . . . 121

5 The paradoxes of set theory: Russell's paradox and others **123**
5.0.6 The Cantor paradox . . . 123
5.0.7 The Russell paradox . . . 123
5.0.8 The need for Axiomatic Set Theory . . . 125

6 Some more problems **126**

1 Sets

The language of ***sets*** was introduced into mathematics in the 19th century, when the great mathematician ***George Cantor*** (1845-1918) almost single-handedly created ***Set theory***.

You should read the article "A history of set theory", in MacTutor.

Today, set theory is not only an important branch of mathematics, but the foundational pillar on which all of mathematics rests. Most mathematicians no longer ask questions that they used to ask, such as "what is a natural number?", or "what is a real number?", or "what is a function?", because they think that all these objects are just special kinds of sets.

This does not mean that they have answered those questions. It just means that they have reduced those questions to just one question: what is a set? Once you know what a set is, then all the other questions are answered.

As for the fundamental question "what is a set?", I am not going to answer it here. What I am going to do is start telling you about sets, until you get used to working with them and talking about them. The question about the ultimate nature of sets will remain unanswered.

1.1 What kind of thing is a set?

Sets are things that we invent in order to combine several objects and form with them a single thing, so that we can talk about the objects as one thing, a "collective entity".

This "grouping" operation, of forming a single thing out of several things, is something we perform very often, using different words, called "collective nouns", to create these collective objects.

Here are some examples of collective nouns.

1. ***Crowds.*** When you see a number of people standing together and shouting something (say, "long live the Queen"), you create a single thing, called "the crowd", so that, instead of saying

the people are shouting "long live the Queen"

you can use the collective noun "crowd" and say

the crowd is shouting "long live the Queen"

*Notice that "the people" have become a single object, "the crowd". So, instead of using the verb in plural ("the people **are** shouting") when you talk about the people, you use the verb in singular ("the crowd **is** shouting") when we talk about the crowd.*

2. ***Flocks of birds.*** When we see a number of birds flying in formation, we create an entity called "the flock", so that, instead of saying

   I see several birds, and they are flying East,

   we can use the collective noun "flock" and say

   I see a flock of birds, and it is flying East.

   *Notice that "the birds" have become a single object, "the flock". So, instead of using the verb in plural ("the birds **are** flying") when we talk about the birds, we use the verb in singular ("the flock **is** flying") when we talk about the flock.*

3. ***Orchestras.*** When several musicians are playing together, we introduce into our discourse the collective noun "orchestra", so that, instead of saying

   The musicians are playing

   we can use the collective noun "orchestra" and say

The orchestra is playing.

*Once again, "the musicians" have become a single object, "the orchestra". So, instead of using the verb in plural ("the musicians **are** playing") when we talk about the musicians, we use the verb in singular ("the orchestra **is** playing") when we talk about the orchestra.*

4. ***Juries.*** When several people are brought together to sit in judgemebnt and decide if a defendant is guilty, the people are called ***jurors***, and are said to be members of the ***jury***.

   And then, instead of saying things like

   The jurors ***are*** deliberating

   we say

   The jury ***is*** deliberating..

   Once again, when we talk about "the jurors" we use the verb in plural ("are deliberating") but when we talk about "the jury" itself we use the verb in singular ("is deliberating") because the jury is a single object.

5. ***The sets*** $\mathbb{N}$***,*** $\mathbb{Z}$***,*** $\mathbb{Q}$ ***and*** $\mathbb{R}$***.*** When numbers of a certain kind are discussed together, we create entities called $\mathbb{N}$ ("the set of all natural numbers"), $\mathbb{Z}$ ("the set of all natural integers"), $\mathbb{Q}$ ("the set of all rational numbers"), $\mathbb{R}$ ("the set of all real numbers"), so that, instead of saying

   there are infinitely many natural numbers

   we can use the collective noun "$\mathbb{N}$" and say

   the set $\mathbb{N}$ is infinite.

   Similarly, instead of saying

all integers are real numbers,

we can use the collective nouns "$\mathbb{N}$" and "$\mathbb{Z}$" and say

$\mathbb{Z}$ is a subset of $\mathbb{R}$.

And, instead of saying

the rational numbers form an ordered field,

or

the real numbers form a complete ordered field,

we can use the collective nouns "$\mathbb{Q}$", "$\mathbb{R}$" and say

$\mathbb{Q}$ is an ordered field

and

$\mathbb{R}$ is a complete ordered field.

*Notice that "the natural numbers", "the integers", "the rational numbers", and "the real numbers" have become single objecta, "$\mathbb{N}$". "$\mathbb{Z}$". "$\mathbb{Q}$", "$\mathbb{R}$". So, instead of using verbs in plural ("there **are** infinitely many natural numbers", "all integers **are** real numbers", "the real numbers **form**..."), when we talk about the numbers, we use verbs in singular ("the set $\mathbb{N}$ **is** infinite", "$\mathbb{Z}$ **is** a subset of $\mathbb{R}$", "$\mathbb{R}$ **is** a complete ordered field") when we talk about the sets.*

1.1.1 Sets with structure

Most of these collective entities have a ***structure***; that is,

1. The members are not all equal and interchangeable. On the contrary, some play special roles.

2. The pairs of members are not all equal and interchangeable. On the contrary, some pairs of members are different from others.

3. The triples of members are not all equal and interchangeable. On the contrary, some triples of members are different from others.

For example,

1. A flock of birds flying in formation has a special member, the ***leader***. And, even more importantly, each bird has ***neighbors***, that is, a few other birds that are right next to it, to the left or to the right or in front or behind, and the bird communicates with its neighbors. The flock stays in formation because each bird, knowing which way its neighbors are moving, tries to move in the same way. "Being neighbors" is what we have called in these notes a ***binary relation***. If we use "xNy" for "x is a neighbor of y", then the "neighbor" relation N singles out some pairs (x, y) of birds as different from other pairs.

2. A number system such as $\mathbb{N}$, or $\mathbb{Z}$, or $\mathbb{R}$ has

   - special members (1 for $\mathbb{N}$, 0 and 1 for $\mathbb{Z}$ and $\mathbb{R}$),
   - special sets of members (for example, for $\mathbb{Z}$ or for $\mathbb{R}$, the set of all positive members of the set),
   - special pairs of members of the set (for example, for $\mathbb{N}$, $\mathbb{Z}$, or $\mathbb{R}$, the pairs (x, y) such that $x < y$ are different from the other pairs),
   - special triples (x, y, z) of members. (For example, the triples (x, y, z) such that $z = x + y$ play a special role: they determine the operation of ***addition***, in the sense that if you know the set S of all the triples (x, y, z) such that $x + y = z$ then you know the operation of addition, because, if I give you numbers x, y, then you can compute x, y by looking in the set S until you find a triple (x, y, z) that is in S, and then the sum $x + y$ is z.)

1.1.2 How sets are different from other collective entities

Usually, you cannot form collective entities by putting together any objects you want, because the objects have to be related in some way. For example,

- You would never form a "crowd" consisting of yourself, the prime minister of Australia, and five people living in Wyoming. To form a crowd, the people have to be together, doing something together.
- And you would never take a bunch of wolves living in Wyoming together with some other wolves who live in Sweden and call that a "pack". To form a pack, the wolves have to be together, run together, and hunt together.

Sets are different, in that they are collective entities that can be formed to put together into a single object ***any objects you want***. The things you put together to form a set do not have to be related in any way. For example,

1. You can form a set whose members are all the wolves in Wyoming.
2. You can form a set whose members are all the wolves in Wyoming together with all the wolves in Sweden.
3. You can form a set whose members are three wolves you like who live in Wyoming, together with the musicians of the New York Philharmonic, your uncle Billy, the planets Earth, Mars and Jupiter, the numbers 5, 7 and 23, the numbers π and $3+\sqrt{5}$, and all the integers that are larger than 377.

The only thing you need in order to be able to form a set S, is a "membership criterion", i.e., a sentence $C(x)$ that specifies the condition that an object x has to satisfy in order to qualify as a member of the set. And any sentence will do[1].

1.1.3 Terms and sentences with variables: a review

In mathematical writing, there are two kinds of meaningful phrases[2], namely, ***terms*** and ***sentences***.

[1] At least for now. Later we will se that we cannot allow absolutely any sentence, because if you do allow that serious trouble ensues, in the form of the "Russell paradox". So we will have to put some limitations. But we are not there yet.

[2] A "phrase" in a particular language is, according to the dictionary, "a small group of words standing together as a conceptual unit". (The "small group" could be just a single

- Terms are phrases that stand for things or people: for example, "Obama", "Alice", "Ronald Reagan", "the table", "the case where I put my sunglasses yesterday", "$2 + 3$", are terms, because they stand for specific things.[3]

- Sentences are phrases that make an assertion that can be true or false: for example, "cows eat grass", "I have no idea where I left the case where I put my sunglasses yesterday", "the planets move around the Sun", "cows like to attack lions and fight them to death", "$2 + 3 = 5$", "$2 + 3 = 6$, and "every odd number is prime") are sentences. (Actually, "cows eat grass" is true, "the planets move around the Sun" is true, "cows like to attack lions and fight them to death" is false, "$2 + 3 = 5$" is true, "$2 + 3 = 6$" is false, and "every odd number is prime" is true.)

Remark 1. Terms are basically the same as "noun phrases", that is, phrases that can serve as the subject of an "is" sentence. So, for example,

- In the sentence "$2 + 3$ is an odd number", the subject is "$2 + 2$", so "$2 + 2$" is a term.

- In the sentence "the case where I put my sunglasses yesterday is on the table", the subject is "the case where I put my sunglasses yesterday", so "the case where I put my sunglasses yesterday" is a term. □

Terms and sentence can contain variables, that is, letters or expressions that do not stand for a definite object, but represent ***slots*** where the name of a person or object can be inserted. Then, when you actually put specific names of persons or objects in the slots,

- A term has a ***value***, i.e., becomes the name of a specific object.

- A sentence has a ***truth value***, i.e., becomes true or false.

---

word. Most phrases are meaningless. For example, the words "Obama" and "Alice" and the longer phrases "Ronald Reagan", "the table", "the case where I put my sunglasses yesterday", "cows eat grass", "the planets move around the Sun", "cows like to attack lions and fight them to death", "$2 + 3$", "$2 + 3 = 5$", "$2 + 3 = 6$", "every odd number is prime", are all phrases.

[3]These things may be concrete,material objects or people, or abstract entities such as numbers. For example, "$2 + 3$" stands for a number, that happens to be the number 5.

But if you leave some of the the slots unfilled (i.e., if you keep some "free variables") then the terms do not have a definite value and the sentences do not have a truth value. In that case, we say that he term or sentence is meaningless, because it does not stand for a specific object or assertion.

Example 1. The term (i.e., noun phrase) "his mother" contains the possessive adjective "his", which is a variable. If you plug in "Barack Obama" for "his" the term becomes "Barack Obama's mother", which stands for a definite person. (In mathematical language, we would talk about "x's mother". And, again, when we plug in "Barack Obama" for "x" the term becomes "Barack Obama's mother", which stands for a definite person.) □

Example 2. The sentence "he is a friend of mine" contains the pronoun "he". If you do not tell me who "he" is, then I don't know what you are talking about. But if you tell me who "he" is, that is, if you ***assign a value*** to the variable "he" (by saying, for example, that "he" stands for "Bill Clinton") then the sentence becomes "Bill Clinton is a friend of mine", which has a definite truth value. (In mathematical language, we would say "x is a friend of mine", and then, when we plug in "Bill Clinton" for "x", we get when we plug in "Barack Obama" for "x" the term becomes "Barack Obama's mother", which stands for a definite person.) □

Example 3. The term "$x + 3y$" contains the letters "x" and "y". If you do not tell me which numbers the letters x and y stand for, then I cannot make sense of which object (in this case, a number) this term stands for. If, on the other hand, you assign specific values to x and y then I can figure out the value of the term. (For example, if you let $x = 4$, $y = -6$, then I can tell that "$x + 3y$" has the value -14, i.e., that $x + 3y = -14$. □

Example 4. The sentence "$x + 3y > 6$" contains the letters "x" and "y". If you do not tell me which numbers the letters x and y stand for, then I cannot make sense of which assertion the sentence is making, and cannot decide if it is true or false, If, on the other hand, you assign specific values to x and y then I can figure out the truth value of the sentence. (for example, if you let $x = 4$, $y = -6$, then I can tell that "$x + 3y = 6$" has the truth value "false", because $x + 3y = 4 - 3 \times 6 = -14$, and $\sim -14 > 6$. But if $x = 3$ and $y = 2$, then $x + 3y = 9$, and $9 > 6$, so "$x + 3y = 6$" is true.. □

1.1.4 Forming sets

As long as you can write a sentence $C(x)$ about a variable object x, you can form the set

$$\{x : C(x)\}$$

that is, the set of all x for which $C(x)$ is true. And you could give this set a name. For example, suppose you want to form the set $\{x : C(x)\}$ and give it the name S. You would do that by writing

$$\text{Let} \qquad S = \{x : C(x)\}.$$

Let us formulate this rule for forming sets as an axiom:

The naïve axiom of set formation

Given any sentence $C(x)$ having x as an open variable, we can form the set whose members are all the objects x for which $C(x)$ is true.

A name for such a set is

$$\{x : C(x)\}\,.$$

And we read this as

The set of all x such that $C(x)$.

Remark 2. Why did I call the set formation axiom "naïve"? The reason is this: in a few days, we will discover that the set formation axiom, as we have formulated it, causes serious problems that can only be solved by changing the statement of the axiom. Instead of a "naïve" axiom that allows us to take any sentence $C(x)$ whatsovever and form the ser $\{x : C(x)\}$, we will have to adopt a "sophisticated" axiom in which nto all sentences are permitted. □

1.1.5 The membership criterion

Suppose we use the sentence "x is a cow" to form a set, and we want to call this set S. To do this, we would write

$$\text{Let} \quad S = \{\, x : x \text{ is a cow} \,\}\,.$$

This means: "I am creating a new set, the set of all x such that x is a cow, and I am calling this set S." or, in much better English, ***"I am creating a new set, the set of all cows, and I am calling it*** S***"***.

Then we can decide whether or not an object a belongs to the set S (that is, whether or not $a \in S$) by applying the following simple test

1. Find out if a is a cow or not.
2. If a is a cow, then a belongs to S.
3. If a is not a cow, then a does not belong to S.

In other words, the sentence "x is a cow" is the ***membership criterion***, or ***membership condition***, for S. A particular object a belongs to the set $\{\, x : x \text{ is a cow} \,\}$ if a is a cow, and doesn't belong to the set of a is not a cow.

For a general sentence $C(x)$:

Suppose $C(x)$ is a sentence having x as an open variable, and you define a set S by writing

$$\text{Let} \qquad S = \{x : C(x)\}\,.$$

Then

- The sentence $C(x)$ is called the membership criterion, or membership condition, for the set S.
- An object a ***belongs*** to S if $C(a)$ is true, and ***doesn't belong*** to S if $C(a)$ is not true.

1.1.6 Forming sets of members of a given set

Suppose we want to form the set of all natural numbers n that are even, i.e., such that $2|n$, and we want to call this set A.

Then we can say:

$$\text{Let} \qquad A = \{n : n \in \mathbb{N} \wedge 2|n\}\,,$$

and we can also say

$$\text{Let} \qquad A = \{n \in \mathbb{N} : 2|n\}\,.$$

The first ssentence is read as "Let A be the set of all things that are natural numbers and are even", whereas the second sentence is read as "Let A be the set of all natural numbers that are even".

And, clearly, both define the same set.

Suppose U is a set, $C(x)$ is a sentence having x as an open variable, and you define a set S by writing

$$\text{Let} \qquad S = \{\, x : x \in U \wedge C(x) \,\}\,.$$

Then the membership criterion is the sentence "$x \in U \wedge C(x)$".
And you can also write

$$\text{Let} \qquad S = \{\, x \in U : C(x) \,\}\,.$$

Example 5. Suppose the membership criterion $C(x)$ is the sentence "x is a natural number that can be written as the sum of the squares of two natural numbers". Let

$$S = \{x : C(x)\}\,.$$

Clearly, $C(x)$ is the sentence

$$x \in \mathbb{N} \wedge (\exists m \in \mathbb{N})(\exists n \in \mathbb{N}) x = m^2 + n^2 \,,$$

so we could have written the definition of S as follows:

$$S = \{x : x \in \mathbb{N} \wedge (\exists m \in \mathbb{N})(\exists n \in \mathbb{N}) x = m^2 + n^2\} \,,$$

or as

$$S = \{x \in \mathbb{N} : (\exists m \in \mathbb{N})(\exists n \in \mathbb{N}) x = m^2 + n^2\} \,, \tag{1.1}$$

(We read this as "S is the set of all natural numbers x such that there exist natural numbers m, n for which $m^2 + n^2 = x$". And an even better reading is "S is the set of all natural numbers that are the sum of two squares of natural numbers".)

Let us consider several possible values of x, and in each case let us figure out whether this x belongs to the set S.

1. Suppose x is the Math 300 textbook. Then x is a book, not a natural number. So $x \notin S$, that is, x is not a member of S.

2. Suppose $x = 5$. Then x is a natural number. And x is the sum of the squares of two natural numbers, because $x = 2^2 + 1^2$. Therefore x satisfies the criterion for membership in S. So x is a member of S, that is, $x \in S$.

3. Suppose $x = -5$. Then x is not a natural number. So $C(x)$ is not true. That is, x does not satisfy the criterion for membership in S. So x is not a member of S.

4. Suppose $x = 7$. Then x is a natural number. Can x be written as the sum of the squares of two natural numbers? The answer is "no". How do we know that? Well, for example, the only suqares of natural numbers that are less than 7 are 1 and 4. And every sum of two of these squares is diffrent from 7. (Indeed: $1 + 1 = 2$, $1 + 4 = 5$, and $4 + 4 = 9$.) So 7 is not the sum of two squares. So x is not a member of S, that is, $x \notin S$. □

1.1.7 How to read the symbol "$\in$"

How to read the "$\in$" symbol

If S is a set and a is an object, we write

$$a \in S$$

to indicate that a is a member of S.

And we write

$$a \notin S$$

to indicate that a is not a member of S.

The expression "$a \in S$" is read in any of the following ways:

- a belongs to S,
- a is a member of S,
- a is in S.

The expression "$a \notin S$" is read in any of the following ways:

- a does not belong to S,
- a is not a member of S,
- a is not in S.

Remark 3. Sometimes, "$a \in S$" is read as "a belonging to S", or "a in S", rather than "a belongs to S", or "a is in S." For example, if we write

Pick an $a \in S$,

then it would be very bad to say "pick an a belongs to S". But "pick an a belonging to S", or "pick an a in S", is fine. □

Never read "$\in$" as "is contained in", or "is included in". The words "contained" and "included" have different meanings, that will be discussed later.

1.2 When are two sets equal?

As we have explained, sets have ***members***. And, even more importantly, ***knowledge of the members of the set determines the set. Two sets that have the same members are the same set.***

Let us make this precise:

The axiom of set equality

Two sets are equal if and only if they have the same members.

In semiformal language:

If A, B are sets, then $A = B$ if and only if

$$(\forall x)(x \in A \iff x \in B)\,.$$

And, in formal language,

$$(\forall A)(\forall B)\Big(A = B \iff (\forall x)(x \in A \iff x \in B)\Big)\,.$$

Example 6. Let

$$\begin{aligned} A &= \{x \in \mathbb{R} : x \geq 0\}\,, \\ B &= \{x \in \mathbb{R} : (\exists y \in \mathbb{R}) y^2 = x\}\,. \end{aligned}$$

Let us prove that $A = B$.

To prove that $A = B$, we have to prove that $(\forall x)(x \in A \iff x \in B)$.

So, let x be arbitrary. We have to prove that $x \in A \iff x \in B$.

To prove this, we have to prove that $x \in A \implies x \in B$ and that $x \in B \implies x \in A$.

Let us first prove that $x \in A \implies x \in B$.

Assume that $x \in A$.

Then $x \in \mathbb{R}$ and $x \geq 0$. (Reason: "$x \in \mathbb{R} \wedge x \geq 0$" is the membership criterion for A.)

But every nonnegative real number has a square root.

So x has a square root. That is, $(\exists y \in \mathbb{R}) y^2 = x$.

So x satisfies the membership criterion for B.

Hence $x \in B$.

Therefore $x \in A \implies x \in B$.

We now prove that $x \in B \implies x \in A$.

Assume that $x \in B$.

Then $x \in \mathbb{R}$ and $(\exists y \in \mathbb{R}) y^2 = x$. (Reason: "$x \in \mathbb{R} \wedge (\exists y \in \mathbb{R}) y^2 = x$" is the membership criterion for B.)

Pick $y \in \mathbb{R}$ such that $y^2 = x$.

Then $y^2 \geq 0$. (Reason: $(\forall u \in \mathbb{R}) u^2 \geq 0$.)

So $x \geq 0$.

So x satisfies the membership criterion for A.

Hence $x \in A$.

Therefore $x \in B \implies x \in A$.

So $x \in A \iff x \in B$. Since x is arbitrary, we can conclude that

$$(\forall x)(x \in A \iff x \in B)\,.$$

Hence $A = B$. **Q.E.D.**

Example 7. Let

$$\begin{aligned} A &= \{x \in \mathbb{R} : x > 0\}, \\ B &= \{x \in \mathbb{R} : (\exists y \in \mathbb{R}) y^2 = x\}. \end{aligned}$$

Let us prove that $A \neq B$.

To prove that $A \neq B$, we have to prove that it is not true that $(\forall x)(x \in A \iff x \in B)$.

Suppose[4] $(\forall x)(x \in A \iff x \in B)$.

Then we can specialize to $x = 0$, and conclude that $0 \in A \iff 0 \in B$.

But "$0 \in B$" means that "$(\exists y \in \mathbb{R}) y^2 = 0$, which is true, because $7^2 = 0$.

On the other hand, "$0 \in A$" means that "$0 > 0$", which is false.

Hence it is not true that $0 \in A \iff 0 \in B$.

So $(0 \in A \iff 0 \in B) \wedge \Big(\sim (0 \in A \iff 0 \in B) \Big)$, which is a contradiction .

Hence $A \neq B$. **Q.E.D.**

Example 8. Let $A = \{n \in \mathbb{Z} : 6|n\}$, and let $B = \{n \in \mathbb{Z} : 2|n \wedge 3|n\}$.

Let us prove that $A = B$.

To prove that $A = B$, we have to prove that $(\forall x)(x \in A \iff x \in B)$.

So, let x be arbitrary. We have to prove that $x \in A \iff x \in B$.

To prove this, we have to prove that $x \in A \implies x \in B$ and that $x \in B \implies x \in A$.

Let us first prove that $x \in A \implies x \in B$.

Assume that $x \in A$.

Then $x \in \mathbb{Z}$ and $6|x$.

Since $6|x$, we may pick $k \in \mathbb{Z}$ such that $x = 6k$.

[4] A proof by contradiction , of course.

Then $x = 2 \times (3k)$, and $3k \in \mathbb{Z}$, so $2|x$.

Also, $x = 3 \times (2k)$, and $2k \in \mathbb{Z}$, so $3|x$.

Hence $2|x \wedge 3|x$.

So $x \in B$.

Therefore $x \in A \Longrightarrow x \in B$.

We now prove that $x \in B \Longrightarrow x \in A$.

Assume that $x \in B$.

Then $x \in \mathbb{Z}$, $2|x$, and $3|x$.

Since $2|x$, we may pick $j \in \mathbb{Z}$ such that $x = 2j$.

Since $3|x$, we may pick $k \in \mathbb{Z}$ such that $x = 3k$.

Then $x = 1.x = (3-2)x = 3x-2x = 3\times(2j)-2\times(3k) = 6(j-k)$.

So $6|x$.

Hence $x \in A$.

Therefore $x \in B \Longrightarrow x \in A$.

So $x \in A \Longleftrightarrow x \in B$. Since x is arbitrary, we can conclude that $(\forall x)(x \in A \Longleftrightarrow x \in B)$. Hence $A = B$. **Q.E.D.**

Problem 1. Let

$$\begin{aligned} A &= \{x \in \mathbb{R} : x^3 > x\}, \\ B &= \{x \in \mathbb{R} : -1 < x < 0 \vee x > 1\} \\ C &= \{x \in \mathbb{R} : -1 < x\}. \end{aligned}$$

Prove or disprove each of the following:

- $A = B$,
- $A = C$.

1.2.1 Subsets

Definition 1. Let A, B be sets. We say that A is a subset of B, and write

$$A \subseteq B\,,$$

if every member of A is a member of B.

In semiformal language, A is a subset of B if and only if

$$(\forall x)(x \in A \Longrightarrow x \in B)\,.$$

In completely formal language:

$$\boxed{(\forall A)(\forall B)\Big(A \subseteq B \Longleftrightarrow (\forall x)(x \in A \Longrightarrow x \in B)\Big)\,.}\ \square$$

Example 9. The following are true:

- $\mathbb{N} \subseteq \mathbb{Z}$,
- $\mathbb{Z} \subseteq \mathbb{Q}$,
- $\mathbb{Q} \subseteq \mathbb{R}$,
- $\{x \in \mathbb{R} : 0 < x < 1\} \subseteq \{x \in \mathbb{R} : 0 \leq x \leq 1\}$. $\square$

Example 10.

The following are true:

- $\{x \in \mathbb{R} : -1 < x < 0\} \subseteq \{x \in \mathbb{R} : x^3 > x\}$.
- $\{n \in \mathbb{N} : n \text{ is prime} \wedge n \neq 2\} \subseteq \{n \in \mathbb{N} : 2|n-1\}$.
- $\{n \in \mathbb{Z} : 4|n\} \subseteq \{n \in \mathbb{Z} : 2|n\}$,
- $\{x \in \mathbb{R} : 0 < x < 1\} \subseteq \{x \in \mathbb{R} : 0 \leq x \leq 1\}$, $\square$

WARNING!

"is a subset of" is a ***binary relation***. It does not make sense to say things like "A is a subset". What does make sense is to say "A is a subset of B".
If, in an exam, I ask you to define "subset", and you say "a set A is a subset if ....", then that is completely wrong and you get zero credit[a]
The definition of "subset" must start with the words: "Let A, B be sets. We say that A is a subset of B if ....

[a] And if your definition starts with horrendous words "subset is when ..." then you lose $10,000,000$ points, on a scale from 0 to 10.

THE SYMBOL "$\not\subseteq$"

The symbol "$\not\subseteq$" means "is not a subset of". So, for example, the following sentences are true:

$$\begin{aligned} \mathbb{R} &\not\subseteq \mathbb{Q}\,, \\ \mathbb{Z} &\not\subseteq \mathbb{N}\,, \\ \{x \in \mathbb{R} : 0 \leq x\} &\not\subseteq \{x \in \mathbb{R} : 0 < x\}\,. \end{aligned}$$

ALWAYS UNDERLINE THE DEFINIENDUM

In a definition, the term being defined is called the definiendum. The definiendum must always be underlined, or highlighted in some way, in order to indicate that we are writing a definition of that term, not just making a true statement.
For example:

- If I write "elephants are four-legged animals", then I am making a true statement about elephants.
- If, on the other hand, I write "elephants are four-legged animals", then I am saying that I am defining the word "elephant" to mean "four-legged animal", and this is of course wrong, because "elephant" does not mean "four-legged animal": there are lots of four-legged animals that are not elephants.
- If I write "an even integer is an integer that is divisible by 2", then I am making a true statement. but I am not saying that this is what "even integer" means.
- If I want to explain what "even integer" means, i.e., give a ***definition*** of "even integer", then I have to say "an even integer is an integer that is divisible by 2". By underlining "even integer" I am conveying the message that this is my definition of "even inteeger".
- If in an exam you are asked to give a definition and you do not underline the definiendum, you will lose points.

Question 1. *In the first sentence of the previous box, why is the word "definiendum" underlined?* □

Problem 2. ***Prove*** the four statements of Example 10.

The structure of your proofs should be as follows:

We want to prove that $A \subseteq B$.

For that purpose, we prove that $(\forall x)(x \in A \Longrightarrow x \in B)$.

Let x be arbitrary. We want to prove "$x \in A \Longrightarrow x \in B$".

Assume $x \in A$.

$\vdots$

$x \in B$.

So $x \in A \Longrightarrow x \in B$.

Therefore $(\forall x)(x \in A \Longrightarrow x \in B)$.

So $A \subseteq B$. **Q.E.D.**

Problem 3. ***Prove*** that the binary relation "$\subseteq$" satisfies the following:

$$(\forall A)A \subseteq A\,, \tag{1.2}$$

$$(\forall A)(\forall B)(A \subseteq B \Longrightarrow B \subseteq A)\,, \tag{1.3}$$

$$(\forall A)(\forall B)(\forall C)\Big(\big(A \subseteq B \wedge B \subseteq C\big) \Longrightarrow A \subseteq C\Big)\,,\,. \tag{1.4}$$

(NOTE: Condition (1.2) says that "$\subseteq$" is ***reflexive***. Condition (1.3) says that "$\subseteq$" is ***symmetric***. Condition (1.4) says that "$\subseteq$" is ***transitive***.)

1.2.2 The empty set

An important example of a set is the ***empty set***, that is, the set that has no members at all.

The symbol for the empty set is

$$\emptyset\,.$$

One possible way to define this set is by the following formula:

$$\boxed{\emptyset = \{x : x \neq x\}\,.}$$

This means that the members of $\emptyset$ are the things x that satisfy $x \neq x$. But our Equality Axiom says that $(\forall x)x = x$. So "$x = x$" is true for every x. This means that no x can be a member of $\emptyset$. So, indeed, $\emptyset$ has no members.

Let us make this precise:

Theorem 1. *The empty set has no members. That is.*

$$(\forall x)x \notin \emptyset\,.$$

Proof.

Let x be arbitrary. We want to prove that $x \notin \emptyset$.

Assume[5] that $x \in \emptyset$.

Then x satisfies the membership criterion for $\emptyset$, i.e.,

$$x \neq x\,.$$

But $(\forall x)x = x$, by the Equality Axiom.

So $x = x$, by the rule for using universal sentences.

Therefore $x = x \wedge x \neq x$, which is a contradiction.

So $x \notin \emptyset$.

Therefore $(\forall x)x \notin \emptyset$. **Q.E.D.**

1.2.3 The empty set is a subset of every set

If you have a set A and a subset B of A, and you remove some members from B, producing a subset C of B, then it is clear that C is still a subset of A. This ought to be true even in the extreme case when you remove *all* the members of B, so that C is the empty set. In other words, the empty set should be a subset of A, for every set A.

Let us prove a precise theorem:

[5] A proof by contradiction !.

Theorem 2. *The empty set is a subset of every set. That is,*

$$(\forall A)\emptyset \subseteq A\,.$$

Proof.

Let A be an arbitrary set. We want to prove that $\emptyset \subseteq A$.

Assume[6] that $\emptyset$ is not a subset of A.

That is, assume that it is not true that every member of $\emptyset$ is in A.

That means that some members of $\emptyset$ are not in A.

In other words, there exists an object x such that $x \in \emptyset$ and $x \notin A$.

Pick one such object and call it a.

Then $a \in \emptyset$ and $a \notin A$.

So in particular $a \in \emptyset$.

But we know from Theorem 1 that $(\forall x)x \notin \emptyset$.

So $a \notin \emptyset$.

Hence $a \in \emptyset \wedge a \notin \emptyset$.

So we have proved a contradiction.

Therefore $\emptyset \subseteq A$.

So $(\forall A)\emptyset \subseteq A$. **Q.E.D.**

1.2.4 Sets with one, two, three or four members

If a is any thing, we can form a set that has a as a member, and no other members. This name of this set is

$$\boxed{\{a\}}\,,$$

which we read as "singleton of a."

The precise definition of $\{a\}$ is as follows.

[6] A proof by contradiction !

Definition 2. Let a be any object. Then the singleton of a is the set $\{a\}$ given by

$$\{a\} = \{x : x = a\}\,.$$

In other words: to be a member of the set $\{a\}$ you have to be a. If you are a then you are a member, and if you are not a then you are not a member.

We can do a similar thing with two objects, say a and b. We can form the set $\{a, b\}$ whose members are a, b, and nothing else. The set $\{a, b\}$ is the unordered pair of a and b.

Definition 3. Let a, b be any two objects. Then the unordered pair of a and b is the set $\{a, b\}$ given by

$$\{a, b\} = \{x : x = a \vee x = b\}\,.$$

Definition 4. A two-member set is a set A such that

$$(\exists a)(\exists b)(a \neq b \wedge A = \{a, b\})\,. \tag{1.5}$$

Remark 4. ***Warning:*** The set $\{a, b\}$ is ***not*** necessarily a set with two members. That depends on who a and b are. For example; if a happens to be equal to b, then $\{a, b\}$ has only one member.

What is true is the following statement: *the set $\{a, b\}$ has two members if $a \neq b$, and one member if $a = b$.* □

Naturally, we can do the same things with three, four, or any number of objects. For example:

Definition 5. Let a, b, c be any three objects. Then the unordered triple of a, b and c is the set $\{a, b, c\}$ given by

$$\{a, b, c\} = \{x : x = a \vee x = b \vee x = c\}\,.$$

Definition 6. A three-member set is a set A such that

$$(\exists a)(\exists b)(\exists c)(a \neq b \wedge a \neq c \wedge b \neq c \wedge A = \{a, b, c\})\,. \tag{1.6}$$

Definition 7. Let a, b, c, d be any four objects.

Then the unordered quadruple of a, b, c and d is the set $\{a, b, c, d\}$ given by

$$\{a, b, c, d\} = \{x : x = a \vee x = b \vee x = c \vee x = d\}\,.$$

Definition 8. A four-member set is a set A such that

$$(\exists a)(\exists b)(\exists c)(\exists d)(a \neq b \wedge a \neq c \wedge a \neq d \wedge b \neq c \wedge b \neq d \wedge c \neq dA = \{a, b, c, d\}) . \tag{1.7}$$

And, in principle, you could go on like this and define sets with five members, sets with 6 members, and so on.

But as soon as the number of members gets large, this way of constructing sets becomes very complicated, so it is better to do it differently.

Example 11. Suppose you want to define a set whose members are the first five presidents of the U.S., and call this set A. That's easy to do. We say:

Let $A = \{$George Washington,John Adams,Thomas Jefferson,James Madison,James Monroe$\}$.

Now suppose you want to define a set whose members are the first 30 U.S. presidents, and call this set B. That is going to be much more complicated right? This is so for two reasons:

- Even if you know the names of the first 30 U.S. presidents, writing them down will be a lot of work,
- In addition, it may happen that you do not know the names of all those presidents.

Here is how you can do it. You can say:

Let
$$B = \left\{ x : (\exists j \in \mathbb{N})(j \leq 30 \wedge x = p_j) \right\},$$
where, for each $j \in \mathbb{N}$ such that $j \leq 30$, p_j is the j-th president of the U.S.

This works perfectly! Indeed, let us see what has to be true of an object x for x to qualify as a member of B. If you are given an object x, and you have to decide whether $x \in B$ or not, you have to find out if there exists a natural number j such that $j \leq 30$ and x is the j-th U.S. president. And that's exactly what we want! □

Problem 4. How many members does the set B of Example 11 have?

HINT: The answer is ***not*** 30. If you think that the answer is 30, think again! Go to a history book (or to a history Web site) and read about Grover Cleveland, who was both the 22nd and the 24th president of the United States. □

Problem 5. Let $A = \{1, 2, 3, 4\}$. Write a list of all the subsets of A. (HINT: There are 16 of them.) □

Problem 6. Write a definition, in the style of Example 11, of the set X whose members are the first 325 prime numbers p such that $p - 3$ is divisible by 4. □

1.3 Operations on sets

There are several operations that enable us to construct new sets from given sets.

1.4 The power set of a set

Definition 9. Let A be a set. The power set of A is the set $\mathcal{P}(A)$ given by

$$\mathcal{P}(A) = \{X : X \subseteq A\}.$$

In other words, $\mathcal{P}(A)$ ***(read as "the power set of*** A***") is the set whose members are all the subsets of*** A***.***

The ***membership criterion*** for the power set $\mathcal{P}(A)$ is the sentence "$X \subseteq A$". That is, for an object X to quality as a member of $\mathcal{P}(A)$, it has to be shown that X is a subset of A.

Example 12. If $A = \{1, 2, 3\}$ then

$$\mathcal{P}(A) = \Big\{ \emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\} \Big\}. \tag{1.8}$$

Notice that A is a finite set with 3 members, and $\mathcal{P}(A)$ has turned out to be a finite set with 8 members. ***This is not a coincidence. We will***

prove later that: if A ***is a finite set and*** A ***has*** n ***members, then the power set*** $\mathcal{P}(A)$ ***is a finite set with*** 2^n ***members.*** □

Problem 7. Let $A = \{1, 2, 3, 4\}$. Write a formula similar to (1.8) listing all the members of $\mathcal{P}(A)$.

Problem 8. Let $A = \{\emptyset, \{\emptyset\}\}$. Write a formula similar to (1.8) listing all the members of $\mathcal{P}\Big(\mathcal{P}(A)\Big)$.

1.5 The union of two sets

Definition 10. Let A, B be sets. The union of A and B is the set $A \cup B$ given by

$$A \cup B = \{x : x \in A \vee x \in B\}.$$

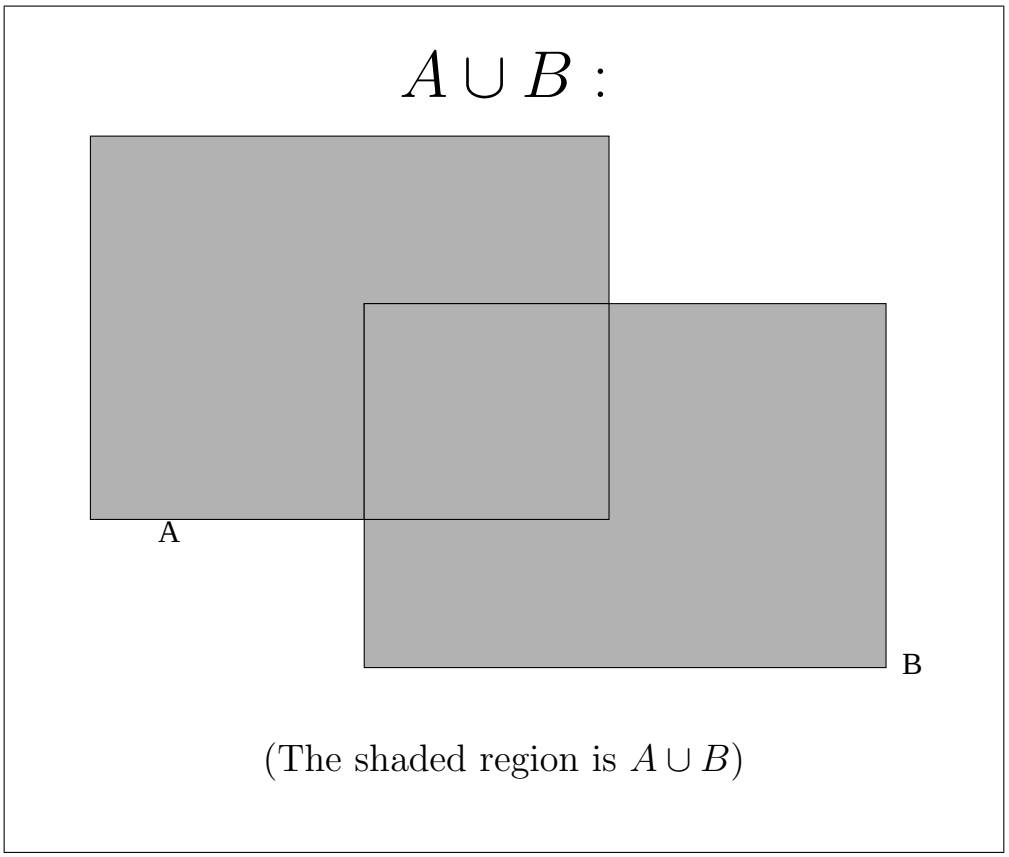
In other words, $A \cup B$ ***(read as "*** A ***union*** B***") is the set whose members are all the members of*** A ***as well as all the members of*** B***.***

The ***membership criterion*** for $A \cup B$ is "$x \in A \vee x \in B$." That is, for an object x to quality as a member of $A \cup B$, it has to be shown that x is in A or that x is in B.

Example 13.

- If $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$ then $A \cup B = \{1, 2, 3, 4\}$.
- If $A = \{a, b, c\}$ and $B = \{d, e, f, g, h, i, j\}$ then $A \cup B = \{a, b, c, d, e, f, g, h, i, j\}$. *Notice that*
  1. *A is a finite set with 3 members,*
  2. *B is a finite set with 7 members,*
  3. *A and B have no memebrs in common (that is, using the terminology of the next section, $A \cap B = \emptyset$),*
  4. *and $A \cup B$ has turned out to be a finite set with 10 members.* ***This is not a coincidence. We will prove later that: if*** A***,*** B ***are finite sets,*** A ***has*** m ***members,*** B ***has*** n ***members, and*** $A \cap B = \emptyset$***, then the union*** $A \cup B$ ***is a finite set with*** $m + n$ ***members.***

5. *If* $A = \{n \in \mathbb{Z} : n > 0\}$ *and* $B = \{n \in \mathbb{Z} : n < 0\}$ *then* $A \cup B = \{n \in \mathbb{Z} : n \neq 0\}$.
6. $\mathbb{N} \cup \{0\}$ *is the set of all nonnegative integers, i.e., the set* $\{n \in \mathbb{Z} : n \geq 0\}$.
7. *If* $A = \{x \in \mathbb{R} : 0 < x < 1\}$ *and* $B = \{x \in \mathbb{R} : 1 \leq x < 2\}$ *then* $A \cup B = \{x \in \mathbb{R} : 0 < x < 2\}$.
8. *If* $A = \{x \in \mathbb{R} : 0 < x < 1\}$ *and* $B = \{x \in \mathbb{R} : 1 < x < 2\}$ *then* $A \cup B = \{x \in \mathbb{R} : 0 < x < 2 \wedge x \neq 1\}$. □



1.6 The intersection of two sets

Definition 11. Let A, B be sets. The intersection of A and B is the set $A \cap B$ given by

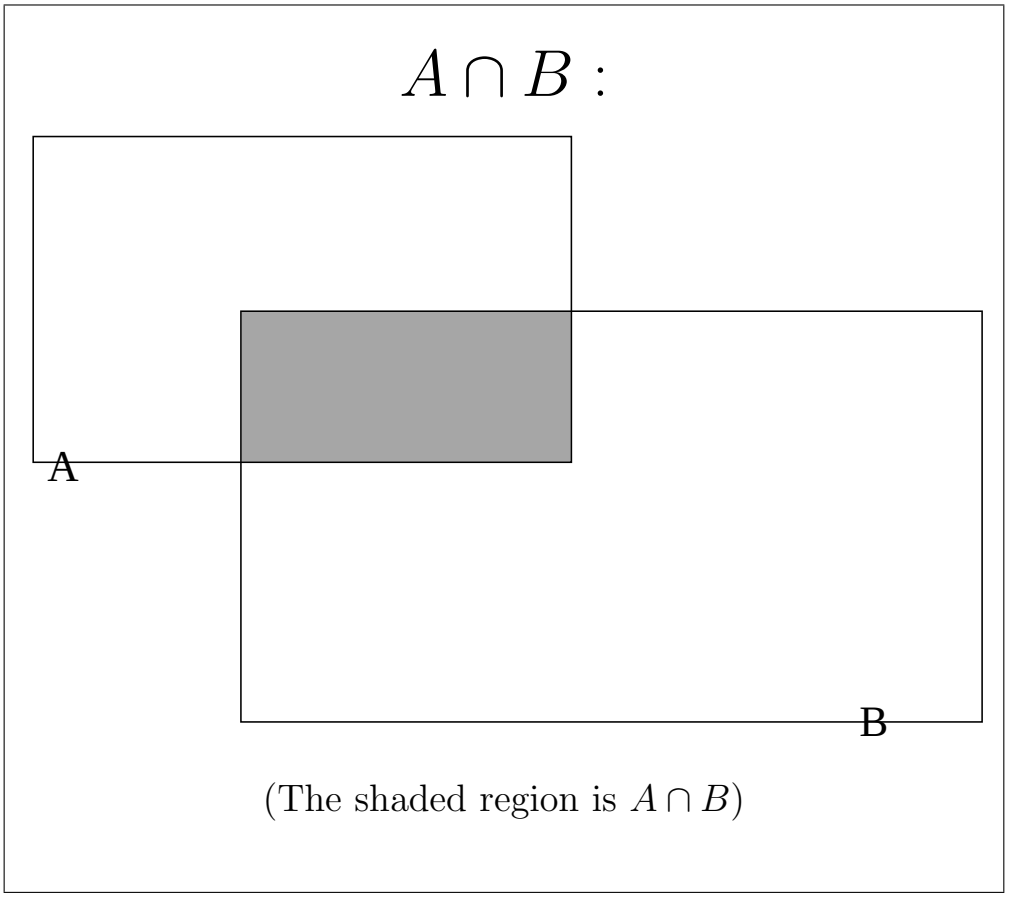
$$A \cap B = \{x : x \in A \wedge x \in B\}.$$

In other words, $A \cap B$ ***(read as "A intersection B") is the set whose members are all the things that belong both to A and to B.***

The ***membership criterion*** for $A \cap B$ is "$x \in A \wedge x \in B$." That is, for an object x to quality as a member of $A \cap B$, it has to be shown that x is in A and that x is in B.

Example 14.

- If $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$ then $A \cap B = \{2, 3\}$.
- If $A = \{n \in \mathbb{Z} : n > 0\}$ and $B = \{n \in \mathbb{Z} : n < 0\}$ then $A \cap B = \emptyset$.
- If $A = \{x \in \mathbb{R} : 0 < x < 2\}$ and $B = \{x \in \mathbb{R} : 1 < x < 3\}$ then $A \cap B = \{x \in \mathbb{R} : 1 < x < 2\}$.



1.7 The difference of two sets

Definition 12. Let A, B be sets. The difference of A and B is the set $A - B$ given by

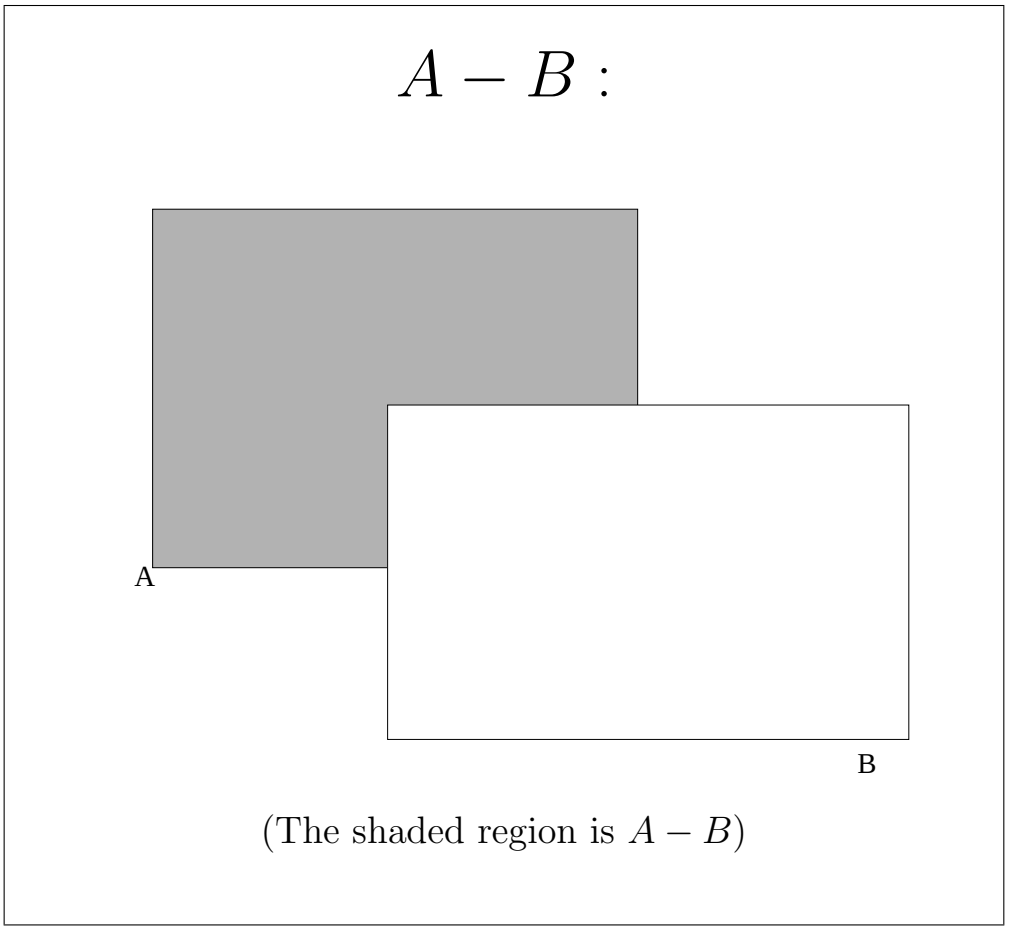
$$A - B = \{x : x \in A \wedge x \notin B\}.$$

In other words, $A - B$ ***(read as "A minus B") is the set whose members are all the things that belong to A but do not belong to B.***

The ***membership criterion*** for $A - B$ is "$x \in A \wedge x \notin B$." That is, for an object x to quality as a member of $A - B$, it has to be shown that x is in A and that x is not in B.

Example 15.

- If $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$ then $A - B = \{1\}$.
- If $A = \mathbb{Z}$ and $B = \mathbb{N}$ then $A - B = \{n \in \mathbb{Z} : n \geq 0\}$.
- If $A = \{x \in \mathbb{R} : 0 < x < 2\}$ and $B = \{x \in \mathbb{R} : 1 < x < 3\}$ then $A - B = \{x \in \mathbb{R} : 0 < x \leq 1\}$.



1.8 Complements

As you may have noticed, the operations of union and intersection are cloely related to the logical connectives $\vee$ and $\wedge$:

$A \cup B$ is the set of those x such that $x \in A \vee x \in B$

$A \cap B$ is the set of those x such that $x \in A \wedge x \in B$

Given this, which is rhe set operation that corresponds to the negation symbol $\sim$? Since $\sim$ is a unary connective (i.e., it can be applied to one sentence S to produce the sentence $\sim S$. the corresponding operation, let us call it $\#$, should be a unary operation defined as follows:

$\#A$ is the set of those x such that $\sim x \in A$.

In other words, $\#A$ should be the set of all the things that are not members of A. This set $\#A$ could be called the "complement" of A, and would be defined by $\#A = \{x : x \notin A\}$.

Now, the set $\#A$ would be truly huge. For example, if $A = \{1, 2, 3, 4\}$, then $\#A$ would consist of all the things other than the numbers $1, 2, 3, 4$. So the members of $\#A$ would be the natural numbers other than $1, 2, 3, 4$ (that is, $5, 6, 7$ and so on), as well as the integers that are not natural numbers, all the real numbers other than $1, 2, 3, 4$, plus all the other things that are not the numbers $1, 2, 3, 4$, that is, all the cows, sheep, giraffes, people, rocks, tables, planets, stars, cells, viruses, molecules, atoms, electrons, protons, quarks, black holes, books, teeth, jackets, socks, cars, planes, forks, knives, and on and on and on.

Usually, when we are doing mathematics, we are studying a specific "universe" of mathematical objects. For example, when we do number theory we study the natural numbers or the integers, when we do Calculus we work with the real nunbers, and when we do Multivariable Calculus we work with $\mathbb{R}^2$, the set of pairs of real numbers)(i.e., the "xy plane") or $\mathbb{R}^3$ (the set of triples (x, y, z) of real numbers, i.e., "3-dimensional space"). If, for example, our "world" is $\mathbb{R}$, then when we have a set A of real numbers, i.e., a subset A of $\mathbb{R}$, we would be interested in the set of real numbers that are not in A. And this set is the difference $\mathbb{R} - A$. Se we give the following definition:

Definition 13. Suppose U is a set that we regard as the "universe", in the sense that we are only interested in sets that are subsets of U. Then the complement of a set A such that $A \subseteq U$ is the set A^c given by

$$A^c = U - A\,, \tag{1.9}$$

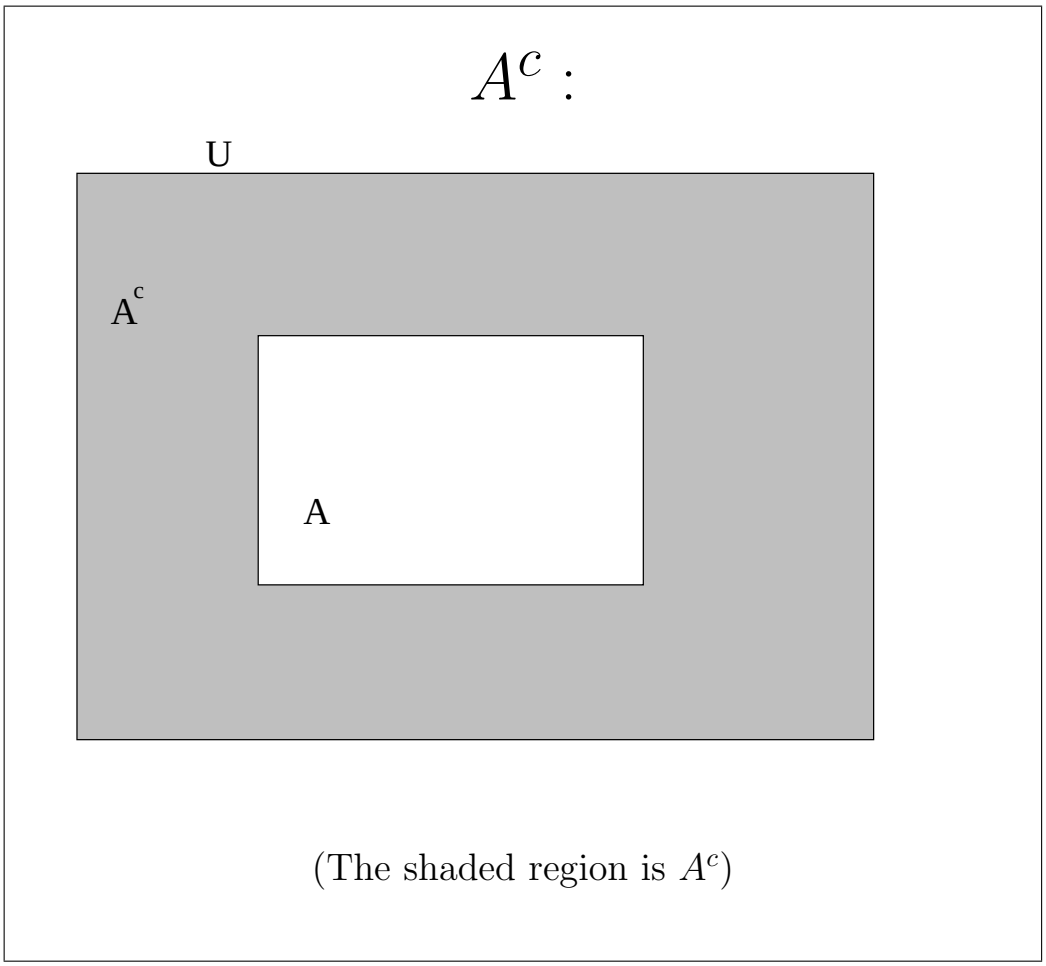
that is,

$$A^c = \{x : x \in U \wedge x \notin A\}\,. \tag{1.10}$$

Remark 5. Strictly speaking, it is inappropriate to define a set as we did in Definition 13 and call it "A^c". This set depends very much on who U is, so

the right thing to do would be to call it the ***complement of*** A ***relative to*** A, and give it a name such as $A^{c,U}$, which shows that the set depends on U.

But, as long as we are working with a fixed "universe", and it is clear who U is, it is O.K. to use a notation such as A^c. □



1.9 The symmetric difference of two sets

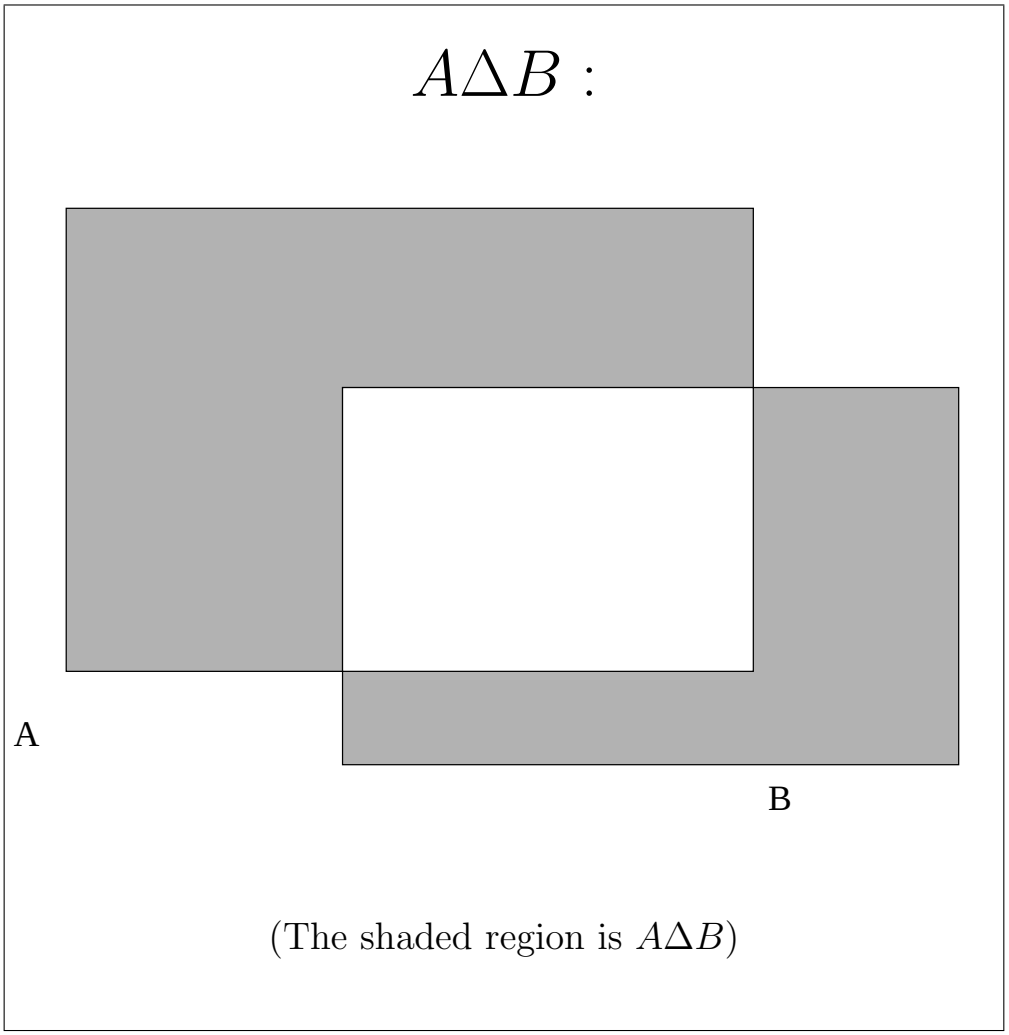
Definition 14 Let A, B be sets. The symmetric difference of A and B is the set $A\Delta B$ given by

$$A\Delta B = \{x : (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)\}.$$

In other words, $A\Delta B$ ***(read as "the symmatric difference of*** A ***and*** B***") is the set whose members are all the things that belong to*** A ***but do not belong to*** B***, or belong to*** B ***but do not belomng to*** A***.***

That is, $A\Delta B$ ***is the set of all things that belong to one of the sets*** A***,*** B ***but do not belong to both.***

The ***membership criterion*** for the symmetric difference $A\Delta B$ is the sentence "$(x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)$". That is, for an object x to quality as a member of $A - B$, it has to be shown that x is in A and that x is not in B, or that x is in B but not in A.



Example 16.

- If $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$ then $A\Delta B = \{1, 4\}$.
- If $A = \{x \in \mathbb{R} : |x| > 4\}$ and $B = \{x \in \mathbb{R} : |x| < 10$ then $A\Delta B = \{x \in \mathbb{R} : |x| \geq 10 \vee |x| \leq 4\}$.

1.10 The Cartesian product of two sets

1.10.1 Ordered pairs

If a, b are any two objects, we would like to have a set, called "the ordered pair of a and b", such that wknowing this set would tell us who a is and who b is, so we would be able to say things such as "the first coordinate of (a, b) is a" and "the second coordinate of (a, b) is b".

For example, suppose we are doing plane geometry, using the standard procedure of drawing and "x axis" and a "y axis", and then representing each point P of the plane by a pair (a, b) of numbers, called the "coordinate pair" of P. Each point P then has, attached to it, a coordinate pair (a, b) of real numbers: the number a is the x ***coordinate*** (or "abscissa") and the number b is the y ***coordinate*** (or "ordinate") of P.

We would like the pair (a, b) to be a set, constructed somehow from a and b. And then the natural question is: which set is the pair (a, b)?

The most naïve idea is to let the pair (a, b) be the unordered pair $\{a, b\}$, that is, the set whose members are a and b.

But this will not do. If we take (a, b) to be $\{a, b\}$, then it cannot happen, for example, that the x-coordinate of $(1, 2)$ is 1, and the x-coordinate of $(2, 1)$ is 2, because, if $(1, 2) = \{1, 2\}$ and $(2, 1) = \{2, 1\}$, then $(1, 2) = (2, 1)$, so, if

(*) the x-coordinate of $(2, 1)$ is 2,

then it would also be true that

(**) the x-coordinate of $(1, 2)$ is 2,

(because $(1, 2) = (2, 1)$), but on the other hand

(***) the x-coordinate of $(1, 2)$ is 1,

so we would get $1 = 2$, which is definitely not true.

The only solution is to define the ordered pair to be something other than the unordered pair $\{a, b\}$. And then the question is, ***what set shall*** (a, b) ***be?***

There are many ways to answer this question, and it really makes no difference which one we use. So we shall choose one, but you must be warned that the specific way we make this choce is not important. What is important is that the following fact is true:

Theorem 3. *Let a, b, c, d be any objects. Then, if the pairs (a, b) and (c, d) are equal, that is, if $(a, b) = (c, d)$, it follows that $c = a$ and $d = b$.*

This is exactly the property that we need. For example, the pairs $(2,1)$ and $(1,2)$ are ***not*** equal. (Proof: Suppose $(2,1) = (1,2)$. Then Theorem 3 (with $a = 2$, $b = 1$, $c = 1$, and $d = 2$, would imply that $2 = 1$. But $2 \neq 1$. So $2 = 1 \wedge 2 \neq 1$, which is a contradiction. So $(2,1) \neq (1,2)$.)

Now we show how to define (a, b) in such a way that Theorem 3 is true.

Definition 15. Let a, b be any two objects. Then the ordered pair of a and b is the set (a, b) given by

$$(a, b) = \{\, \{a\}\,,\, \{a, b\}\,\}\,. \tag{1.11}$$

Proof of Theorem 3. Suppose that $(a, b) = (c, d)$.
Let $p = (a, b)$, so p is also equal to (c, d) because we are assuming that $(a, b) = (c, d)$.
Since $p = \{\, \{a\}, \{a, b\}\,\}$, the set p has either two members (if $b \neq a$) or one member (if $a = b$, in which case $\{a, b\} = \{a\}$, so $\{\, \{a\}, \{a, b\}\,\} = \{\, \{a\}, \{a\}\,\} = \{\, \{a\}\,\}$).
But in either case, a is the only object that belongs to all the members of p.
And, since p is also equal to (c, d), it follows that c is the only object that belongs to all the members of p.
So $\boxed{\boxed{c = a}}$.
Next, let us prove that $d = b$.
We consider separately the two possible cases: $b = a$ and $b \neq a$.

> Assume that $b = a$.
>
> Then p has only one member, because, as explained before, $\{a, b\} = \{a\}$, so $p = \{\, \{a\}, \{a, b\}\,\} = \{\, \{a\}\,\}$.
>
> But then (c, d) also has only one member, because $(c, d) = p$. And this implies that $d = c$.
>
> So $d = c$ and $b = a$, and we already know that $c = a$.
>
> Hence $\boxed{d = b}$.
>
> Now assume that $b \neq a$.
>
> Then the sets $\{a\}$ and $\{a, b\}$ are different, because $b \in \{a, b\}$ but $b \notin \{a\}$.

So p has two different members.

And b is the only object that belongs to one of the members of p but does not belong to both.

And, similarly, d is the only object that belongs to one of the members of p but does nto belong to both.

So $\boxed{d = b}$.

We have proved that $d = b$ in both cases, when $b = a$ and when $b \neq a$.
So $\boxed{\boxed{d = b}}$.

So we have proved that $\boxed{\boxed{\boxed{c = a \wedge d = b}}}$. **Q.E.D.**

1.10.2 The Cartesian product of two sets

Definition 16. Let A, B be sets. The Cartesian product of A and B is the set $A \times B$ given by

$$A \times B = \left\{ u : (\exists a)(\exists b)(a \in A \wedge b \in B \wedge u = (a, b)) \right\}.$$

In other words, $A \times B$ (read as "A times B") is the set of all objects u such that u is an ordered pair (a, b), with $a \in A$ and $b \in B$.

Or, more succintly and elegantly, $A \times B$ ***is the set of all ordered pairs*** (a, b) ***for which*** $a \in A$ ***and*** $b \in B$.

Example 17.

- Let $A == \{1, 2, 3\}$ and $B = \{2, 3, 4, 5\}$. Then

$$\begin{aligned} A \times B \;\; = \;\; \Big\{ & (1,2), (1,3), (1,4), (1,5), (2,2), (2,3), (2,4), (2,5), \\ & (3,2), (3,3), (3,4), (3,5) \Big\}. \end{aligned}$$

Notice that A is a finite set with 3 members, B is a finite set with 4 members, and $A \times B$ is a finite set with 12 members. ***This is not a coincidence. We will prove later that: if A, B are finite sets, A has m members, and B has n members, then $A \times B$ is a finite set and $A \times B$ has mn members.***

- Let $A = \mathbb{R}$, $B = \mathbb{R}$. Then $A \times B$ is $\mathbb{R} \times \mathbb{R}$, that is, the set of all ordered pairs (x, y) such that x and y are real numbers. ***This is the "x-y plane" of plane Euclidean geometry. The members of $\mathbb{R} \times \mathbb{R}$ are the "points" of plane geometry.***

- Let

$$\begin{aligned} A &= \{x \in \mathbb{R} : 0 < x < 1\}, \\ B &= \{x \in \mathbb{R} : 1 < x < 3\}. \end{aligned}$$

  Then A is the open interval $(0, 1)$ (***not to be confused with the ordered pair*** $(0, 1)$***!***) and B is the open interval $(1, 3)$ (***not to be confused with the ordered pair*** $(1, 3)$***!***). In this case, $A \times B$, that is, $(0, 1) \times (1, 3)$, is the set of all pairs (x, y) of real numbers such that $0 < x < 1$ and $1 < y < 3$. In other words, $(0, 1) \times (1, 3)$ ***is the rectangle R characterized by the inequalities***

$$0 < x < 1 \qquad \text{and} \qquad 1 < y < 3\,.$$

1.11 Important facts about the set operations

So far, we have defined:

- One very special set (the empty set),
- One binary predicate (i.e., relation), about sets, namely, the predicate "is a subset of".
- Five binary operations on sets (union, intersection, difference, symmetric difference, and Cartesian product),
- One unary operation on sets (the power set).

By combining these nine things we can produce an enormous number of possible facts, some of which might be true, while others are not true. It would be pointless for me to give you a complete list and prove them all, because there are so many of them, and they are all so easy to prove (if true) or to disprove (if false).

And it would be pointless for you to memorize them all, because the list is so long. On the other hand, if you understand what you are doing, you ought to be able, in each case, to figure out if the statement is true or false, and how to prove it (if it is true) or disprove it (if it is false).

So what I suggest is this: ***read carefully the list of facts, and pick a few of them and prove them or disprove them. Keep in mind that any of these facts could show up as a question in the exams.***

And here is the list:

1. If A is a set, then $\emptyset \subseteq A$. (True)

2. If A is a set, then $\emptyset \in A$. (False)

3. If A is a set, then $A \cup \emptyset = A$. (True)
   NOTE: If you think that $\emptyset$ is like the number 0, and the operation "$\cup$" is like addition, then this statement is analogous to the statement that $x + 0 = x$ for every real number x.

4. If A is a set, then $A \cup \emptyset = \emptyset$. (False)

5. If A is a set, then $A \cap \emptyset = A$. (False)

6. If A is a set, then $A \cap \emptyset = \emptyset$. (True)
   NOTE: If you think that $\emptyset$ is like the number 0, and the operation "$\cap$" is like multiplication, then this statement is analogous to the statement that $x.0 = 0$ for every real number x.

7. If A is a set, then $A \subseteq A$. (True)

8. If A, B are sets, then $A = B$ if and only if $A \subseteq B \wedge B \subseteq A$. (True)
   NOTE: This gives an another way to prove that two sets are equal: to prove that $A = B$, you prove that $A \subseteq B$ and that $B \subseteq A$.

9. If A is a set, then $A \cup A = A$. (True)

10. If A is a set, then $A \cap A = A$. (True)

11. If A, B are sets, then $A \subseteq A \cup B$. (True)

12. If A, B are sets, then $A \subseteq A \cap B$. (False)

13. If A, B are sets, then $A \cup B \subseteq A$. (False)

14. If A, B are sets, then $A \cap B \subseteq A$. (True)

15. If A is a set, then $A \subseteq A$. (True)
NOTE: This aays that the binary relation "$\subseteq$" is reflexive.

16. If A, B are sets, $A \subseteq B$, and $B \subseteq A$, then $A = B$. (True)
NOTE: This aays that the binary relation "$\subseteq$" is antisymmetric.

17. If A, B, C are sets, $A \subseteq B$, and $B \subseteq C$, then $A \subseteq C$. (True)
NOTE: This aays that the binary relation "$\subseteq$" is transitive.

18. If A, B, C are sets, $A \subseteq B$, $B \subseteq C$, and $C \subseteq A$, then $A = B = C$. (True)

19. If A, B are sets, then $A \subseteq B$ if and only if $A \cup B = B$. (True)

20. If A, B are sets, then $A \subseteq B$ if and only if $A \cup B = A$. (False)

21. If A, B are sets, then $A \subseteq B$ if and only if $A \cap B = A$. (True)

22. If A, B are sets, then $A \subseteq B$ if and only if $A \cap B = B$. (False)

23. If A, B are sets, then $A \cup B = B \cup A$. (True)
NOTE: This is the ***commutative law of the union operation****.*

24. If A, B are sets, then $A \cap B = B \cap A$. (True)
NOTE: This is the ***commutative law of the intersection operation****.*

25. If A, B, C are sets, then $A \cup (B \cup C) = (A \cup B) \cup C$. (True)
NOTE: This is the ***associative law of the union operation****.*

26. If A, B, C are sets, then $A \cap (B \cap C) = (A \cap B) \cap C$. (True)
NOTE: This is the ***associative law of the intersection operation****.*

27. If A, B, C are sets, and $A \subseteq B$, then $A \cup C \subseteq B \cup C$. (True)

28. If A, B, C are sets, and $A \subseteq B$, then $A \cap C \subseteq B \cap C$. (True)

29. If A, B, C are sets, then $(A \cup B) \cap C = A \cup (B \cap C)$. (False)

30. If A, B, C are sets, then $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.(True)
NOTE: This is the ***distributive law of union with respect to intersection****.*

31. If A, B, C are sets, then $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.(True)
NOTE: This is the ***distributive law of intersection with respect to union****.*

    IMPORTANT NOTE: We have seen that union and intersection are in some ways like addition and multiplication: they obey commoutative and associative laws. and also $A \cap \emptyset = \emptyset$ (which is analogous to $x \cdot 0 = 0$) and $A \cup \emptyset = A$ (which is analgous to $x + 0 = x$). But ***the analogy should not be pushed too far:***

    - *there is a distributive law of union with respect to intersection (i.e., $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$),*
    - *and there is also a distributive law of intersection with respect to union (i.e., $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$),*
    - *but this is totally unlike what happens for addition and multiplication, because*
    - *there is a distributive law of multiplication with respect to addition (i.e., $x \cdot (y + z) = x \cdot y + x \cdot z$)*
    - *but there is no distributive law of addition with respect to multiplication (i.e., it is not true that $x + (y \cdot z) = (x + y) \cdot (x + z)$ since, for example, if we take $x = 1$, $y = 2$, $z = 3$, then $x + (y \cdot z) = 7$ and $(x + y) \cdot (x + z) = 12$).*

32. If A, B are sets, then $(A - B) \cup B = A$. (False)

33. If A, B are sets, then $(A - B) \cup B \subseteq A$. (False)

34. If A, B are sets, then $A \subseteq (A - B) \cup B$. (True)

35. If A, B, C are sets, then $A \cup (B - C) = (A \cup B) - (A \cup C)$. (False)

36. If A, B, C are sets, then $A \cap (B - C) = (A \cap B) - (A \cap C)$. (False)

    When we fix a "universe" U, then the complement of a subset A of U is defined to be the set $U - A$. The complement of A is denoted by "A^c".

37. If A, U are sets, and $A \subseteq U$, then $(A^c)^c = A$. (True)

38. If A, U are sets, and $A \subseteq U$, then $A \cup A^c = U$. (True)

39. If A, U are sets, and $A \subseteq U$, then $A \cap A^c == \emptyset$. (True)

40. If A, B, U are sets, $A \subseteq U$, and $B \subseteq U$, then

$$(A \cup B)^c = A^c \cap B^c \,. \tag{1.12}$$

    (This is true.)

41. If A, B, U are sets, $A \subseteq U$, and $B \subseteq U$, then

$$(A \cap B)^c = A^c \cup B^c \,. \tag{1.13}$$

    (This is true.)

    NOTE: Equations (1.12) and (1.13) are the famous ***De Morgan laws****. They say that*

    - ***the complement of the union of two sets is the intersection of the complements of the sets****,*

    and

    - ***the complement of the intersection of two sets is the union of the complements of the sets****.*

    I strongly recommend that you read the article on "De Morgab laws" in Wikipedia.

42. If A, B, U are sets, $A \subseteq U$, and $B \subseteq U$, then $A - B = A \cap B^c$. (True)

43. If A, B are sets, then $A - B = B - A$. (False)

44. If A, B, C are sets, then $A - (B - C) = (A - B) - C$. (False)

45. If A, B are sets, then $A\Delta B = (A \cup B) - (A \cap B)$. (True)
46. If A, B are sets, then $A\Delta B = B\Delta A$. (True)
47. If A, B, C are sets, then $A\Delta(B\Delta C) = (A\Delta B)\Delta C$. (True)
48. If A, B are sets, then $A \times B = B \times A$. (False)
49. If A, B are sets, and $A \times B = B \times A$, then $A = B$. (False)
50. If A, B are nonempty sets, and $A \times B = B \times A$, then $A = B$. (True)
51. If A, B, C, D are sets, then

$$(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)\,.$$

(This is true.)

52. If A, B, C, D are sets, then

$$(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)\,.$$

(This is false.)

53. If A is a set, then $A \in \mathcal{P}(A)$. (True)
54. If A is a set, then $A \subseteq \mathcal{P}(A)$. (False)
55. If A is a set, then $\emptyset \in \mathcal{P}(A)$. (True)
56. If A is a set, then $\emptyset \subseteq \mathcal{P}(A)$. (True)
57. If A, B are sets, then $A \subseteq B$ if and only if $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. (True)
58. If A, B are sets, then $A = B$ if and only if $\mathcal{P}(A) = \mathcal{P}(B)$. (True)
59. If A, B are sets, then $\mathcal{P}(A \times B) = \mathcal{P}(A) \times \mathcal{P}(B)$. (False)
60. If A is a set, then $\emptyset \times A = \emptyset$ and $A \times \emptyset = \emptyset$. (True)

Problem 9. ***Prove*** all the true statements of the list of 60 statements that begins on page 41. and ***disprove*** all false ones. □

1.12 Some examples of proofs about sets

Let me give you the proofs of some of the results in the long list of the previous section.

1.12.1 Proof of one of the distributive laws

Theorem 4. *If A, B, C are sets, then*

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)\,. \tag{1.14}$$

Proof. To prove that the sets $A \cup (B \cap C)$ and $(A \cup B) \cap (A \cup C)$ are equal, we prove that they have the same members, that is, we prove that

$$(\forall x)\Big(x \in A \cup (B \cap C) \iff x \in (A \cup B) \cap (A \cup C)\Big)\,. \tag{1.15}$$

Sentence (1.15) is a universal sentence, of the form $(\forall x)P(x)$. So, in order to prove it, we let x be an arbitrary object and prove $P(x)$.

Let x be arbitrary.

We want to prove

$$x \in A \cup (B \cap C) \iff x \in (A \cup B) \cap (A \cup C)\,. \tag{1.16}$$

(1) The sentence "$x \in A \cup (B \cap C)$" is equivalent to "$x \in A \vee x \in B \cap C$". (Reason: if X, Y are sets, then the criterion for membership in $X \cup Y$ is "$x \in X \vee x \in Y$".)

(2) And "$x \in B \cap C$" is equivalent to "$x \in B \wedge x \in C$". (Reason: if X, Y are sets, then the criterion for membership in $X \cap Y$ is "$x \in X \wedge x \in Y$".)

(3) Hence "$x \in A \cup (B \cap C)$" is equivalent to "$x \in A \vee (x \in B \wedge x \in C)$".

(4) Also, "$x \in (A \cup B) \cap (A \cup C)$" is equivalent to "$x \in A \cup B \wedge x \in A \cup C$".

And

- "$x \in A \cup B$" is equivalent to "$x \in A \vee x \in B$".
- "$x \in A \cup C$" is equivalent to "$x \in A \vee x \in C$".

(5) So "$x \in (A \cup B) \cap (A \cup C)$" is equivalent to "$(x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$".

It follows from (3) and (6) that "$x \in A \cup (B \cap C) \iff x \in (A \cup B) \cap (A \cup C)$", the sentence that we have to prove, is equivalent to

$$x \in A \vee (x \in B \wedge x \in C) \iff \Big((x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \Big) . \tag{1.17}$$

The sentence (1.17) is of the form

$$P \vee (Q \wedge R) \iff \Big(P \vee Q) \wedge (P \vee R) \Big) , \tag{1.18}$$

where P stands for "$x \in A$", Q stands for "$x \in B$", and R stands for "$x \in C$".

We now prove that (1.18) is true.

Sentence (1.18) is a biconditional, of the form $\mathcal{L} \iff \mathcal{M}$. And a biconditional $\mathcal{L} \iff \mathcal{M}$ is true if and only if $\mathcal{L}$ and $\mathcal{M}$ have the same truth value, i.e., are both true or both false. So we are going to prove that $\mathcal{M}$ is true if $\mathcal{L}$ is true and $\mathcal{M}$ is false if $\mathcal{L}$ is false.

Suppose that $P \vee (Q \wedge R)$ is true.

Then either P is true or $Q \wedge R$ is true.

Suppose P is true.

Then both $P \vee Q$ and $P \vee R$ are true.

So $(P \vee Q) \wedge (P \vee R)$ is true.

Now suppose that $Q \wedge R$ is true.

Then both Q and R are true.

So $P \vee Q$ and $P \vee R$ are true.

And then $(P \vee Q) \wedge (P \vee R)$ is true.

So $(P \vee Q) \wedge (P \vee R)$ is true in both cases, and then $(P \vee Q) \wedge (P \vee R)$ is true.

This proves that $(P \vee Q) \wedge (P \vee R)$ is true if $P \vee (Q \wedge R)$ is true.

Now suppose that $P \vee (Q \wedge R)$ is false.

Then both P and $Q \wedge R$ are false.

Since $Q \wedge R$ is false, either Q is false or R is false.

Suppose Q is false.

Since P is false, $P \vee Q$ is false, because both P and Q are false.

Hence the conjunction $(P \vee Q) \wedge (P \vee R)$ is false.

Now suppose R is false.

Since P is false, $P \vee R$ is false, because both P and R are false.

Hence the conjunction $(P \vee Q) \wedge (P \vee R)$ is false.

So $(P \vee Q) \wedge (P \vee R)$ is false in both cases, and then $(P \vee Q) \wedge (P \vee R)$ is false.

This proves that $(P \vee Q) \wedge (P \vee R)$ is false if $P \vee (Q \wedge R)$ is false.

So we have proved that (1.17) is true, and this completes our proof, **Q.E.D.**

Problem 10. ***Prove*** the other distributive law: If A, B, C are sets, then

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)\,. \tag{1.19}$$

1.12.2 Proofs of the De Morgan laws

As we explained before, the De Morgan laws are the following two statements.

Theorem 5. *Let U be a set, and let A, B be subsets of U. Then*

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

and

Theorem 6. *Let U be a set, and let A, B be subsets of U. Then*

$$\begin{aligned}(A \cup B)^c &= A^c \cap B^c\,,\\ (A \cap B)^c &= A^c \cap B^c\,.\end{aligned}$$

I will give you a proof from first principles[7] of the first theorem, and then I will give you a short proof of the other using the first one, and ask you to give a proof from first principles of the second theorem.

Proof. We want to prove that

$$(\forall x \in U)\Big(x \in (A \cup B)^c \iff x \in A^c \cap B^c\Big)\,. \tag{1.20}$$

The sentence we want to prove is a universal sentence, of the form $(\forall x)P(x)$. So in order to prove it we let x be an arbitrary object and prove $P(x)$.

Let x be an arbitrary member of U.

We want to prove that

$$x \in (A \cup B)^c \iff x \in A^c \cap B^c\,. \tag{1.21}$$

But, for $x \in U$, "$x \in (A \cup B)^c$ is equivalent to "$x \notin A \cup B$", i.e., to "$\sim x \in A \cup B$".

And "$x \in A \cup B$" is equiva;ent to "$x \in A \vee x \in B$".

So "$x \notin A \cup B$" is equivalent to "$\sim (x \in A \vee x \in B)$".

Therefore "$x \in (A \cup B)^c$" is equivalent to "$\sim (x \in A \vee x \in B)$".

On the other hand, "$x \in A^c \cap B^c$" is equiva;ent to "$x \in A^c \wedge x \in B^c$".

And the sentences "$x \in A^c$", "$x \in B^c$" are equivalent to "$\sim x \in A$" and "$\sim x \in B$".

So "$x \in A^c \cap B^c$" is equivalent to "$(\sim x \in A) \wedge (\sim x \in B)$".

Hence (1.21) is equivalent to

$$\Big(\sim (x \in A \vee x \in B)\Big) \iff \Big((\sim x \in A) \wedge (\sim x \in B)\Big)\,. \tag{1.22}$$

[7] A ***proof from first principles*** is a proof in which you do not use any intermediate results proved before. For example, after we proved that $2 + 2 = 4$ from first principles we proved that $2 \times 2 = 4$ using the result that $2 + 2 = 4$. That was ***not*** a proof from first principles. In a proof from first principles, you would just have used the basic facts and the definitions, and no theorem proved before.

If we use P to stand for "$x \in A$", and Q to stand for "$x \in B$", then (1.22) is the sentence

$$\Big(\sim (P \vee Q) \Big) \iff \Big((\sim P) \wedge (\sim Q) \Big) . \tag{1.23}$$

The biconditional sentence (1.23) is of the form $\mathcal{L} \iff \mathcal{M}$. And a biconditional $\mathcal{L} \iff \mathcal{M}$ is true if and only if $\mathcal{L}$ and $\mathcal{M}$ have the same truth value, i.e., are both true or both false. So we are going to prove that $\mathcal{M}$ is true if $\mathcal{L}$ is true and $\mathcal{M}$ is false if $\mathcal{L}$ is false.

Proof that if $\sim (P \vee Q)$ *is true then* $(\sim P) \wedge (\sim Q)$ *is true.*

Suppose that $\boxed{\sim (P \vee Q) \text{ is true}}$.

Then $P \vee Q$ is false.

So both P and Q are false.

Hence $\sim P$ and $\sim Q$ are true.

So the conjunction $\boxed{(\sim P) \wedge (\sim Q) \text{ is true}}$.

Proof that if $\sim (P \vee Q)$ *is false then* $(\sim P) \wedge (\sim Q)$ *is false.*

Suppose that $\boxed{\sim (P \vee Q) \text{ is false}}$.

Then $P \vee Q$ is true.

So either P is true or Q is true.

> Suppose that P is true.
> Then $\sim P$ is false.
> So the conjunction $(\sim P) \wedge (\sim Q)$ is false.
> Now suppose that Q is true.
> Then $\sim Q$ is false.
> So the conjunction $(\sim P) \wedge (\sim Q)$ is false.

We have shown that $(\sim P) \wedge (\sim Q)$ is false in both cases, when P is true and when Q is true.

Hence $\boxed{(\sim P) \wedge (\sim Q) \text{ is false}}$.

So we have proved (1.21) for an arbitrary member x of U, and we can go to

$$(\forall x \in U) \Big(x \in (A \cup B)^c \iff x \in A^c \cap B^c \Big) . \tag{1.24}$$

And (1.24) says that the sets $(A \cup B)^c$ and $(A \cap B)^c$ have rhe same members, so the sets are equal, that is

$$(A \cup B)^c = A^c \cap B^c \,. \tag{1.25}$$

This is exactly what we wanted to prove. **Q.E.D.**

Now let us give a simple proof of Theorem 6 using Theorem 5.

Proof. We want to prove that

$$(A \cap B)^c = A^c \cup B^c. \tag{1.26}$$

Theorem 5 says that, if X, Y are any subsets of U, then

$$(X \cup Y)^c = X^c \cap Y^c \,. \tag{1.27}$$

Apply this with $X = A^c$ and $B = Y^c$. We get

$$(A^c \cup B^c)^c = (A^c)^c \cap (B^c)^c \,. \tag{1.28}$$

But $(A^c)^c = A$, and $(B^c)^c = B$. So

$$(A^c \cup B^c)^c = A \cap B \,. \tag{1.29}$$

Now take the complement of both sides. We get

$$\Big((A^c \cup B^c)^c\Big)^c = (A \cap B)^c \,. \tag{1.30}$$

But $(X^c)^c = X$ for every subset X of U. Therefore

$$\Big((A^c \cup B^c)^c\Big)^c = A^c \cup B^c \tag{1.31}$$

Combining (1.30) and (1.31), we get

$$A^c \cup B^c c = (A \cap B)^c \,, \tag{1.32}$$

which is the formula we were trying to prove. **Q.E.D.**

Problem 11. Write a proof from first principles[8] of Theorem 6. ***I strongly recommend that you use the same style as in the proof of Theorem 5. The proof of Theorem 5 is really very simple, and almost mechanical. It looks long because it was written on purpose to show you a proof written in a very precise, very detailed way, displaying the use of the rules of logic. Usually one does not write p;roofs like that, but I would like you to do it at least once, to show that you can do it.*** □

1.12.3 A proof involving the symmetric difference

Let us prove Fact 45 from our list. Recall that the ***symmetric difference*** of two sets A, B is the set $A\Delta B$ given by

$$A\Delta B = (A - B) \cup (B - A)\,.$$

In the proof, we are going to use the following facts, that are valid for arbitrary subsets X, Y, Z of a set U:

- $X - Y = X \cap Y^c$,
- $X \cup X^c = U$ and $X \cap X^c = \emptyset$,
- $X \cap U = X$ and $X \cap \emptyset = \emptyset$.
- $X \cup U = U$ and $X \cup \emptyset = X$.
- The commutative laws

$$\begin{aligned} X \cup Y &= Y \cup X\,, \\ X \cap Y &= Y \cap X\,, \end{aligned}$$

- The associative laws

$$\begin{aligned} X \cup (Y \cup Z) &= (X \cup Y) \cup Z\,, \\ X \cap (Y \cap Z) &= (X \cap Y) \cap Z\,, \end{aligned}$$

[8] "From first priciples" means "not using other theorems proved before". In our case, this means "not using Theorem 5".

- The distributive laws

$$\begin{aligned} X \cup (Y \cap Z) &= (X \cup Y) \cap (X \cup Z), \\ X \cap (Y \cup Z) &= (X \cap Y) \cup (X \cap Z), \end{aligned}$$

- The De Morgan laws

$$\begin{aligned} X^c \cup Y^c &= (X \cap Y)^c, \\ X^c \cap Y^c &= (X \cup Y)^c. \end{aligned}$$

Theorem 7. *If A, B are sets, then $A\Delta B = (A \cup B) - (A \cap B)$.*

Proof. Choose as universe any set U such that $A \subseteq U$ and $B \subseteq U$. (For example, we could choose U to be $A \cup B$.)

Then

$$\begin{aligned} A\Delta B &= (A - B) \cup (B - A) && (1.33)\\ &= (A \cap B^c) \cup (B \cap A^c) && (1.34)\\ &= \Big((A \cap B^c) \cup B\Big) \cap \Big((A \cap B^c) \cup A^c\Big) && (1.35)\\ &= \Big(B \cup (A \cap B^c)\Big) \cap \Big(A^c \cup (A \cap B^c)\Big) && (1.36)\\ &= \Big((B \cup A) \cap (B \cup B^c)\Big) \cap \Big((A^c \cup A) \cap (A^c \cup B^c)\Big) && (1.37)\\ &= \Big((B \cup A) \cap U\Big) \cap \Big(U \cap (A^c \cup B^c)\Big) && (1.38)\\ &= (B \cup A) \cap (A^c \cup B^c) && (1.39)\\ &= (A \cup B) \cap (A^c \cup B^c) && (1.40)\\ &= (A \cup B) \cap (A \cap B)^c. && (1.41) \end{aligned}$$

So $A\Delta B = (A \cup B) - (A \cap B)$. **Q.E.D.**

Problem 12. Write the justfications of each of the nine steps (1.33), (1.34), (1.35), (1.36), (1.37), (1.38), (1.39), (1.40), (1.41) of the proof of Theorem 7. □

Problem 13. ***Prove or disprove*** each of the following distributive laws

1. *The distributive law of intersection with respect to symmetric difference.* If A, B, C are sets, then

$$A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C) \,. \tag{1.42}$$

2. *The distributive law of union with respect to symmetric difference.* If A, B, C are sets, then

$$A \cup (B \Delta C) = (A \cup B) \Delta (A \cup C) \,. \tag{1.43}$$

2 Relations and functions

2.1 The definition of "relation"

Definition 17. A relation is a set of ordered pairs.

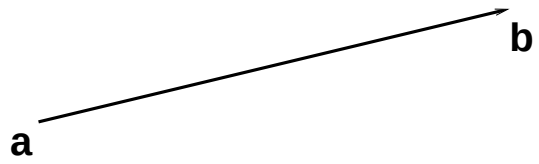
That is:
A relation is a set R such that every member of R is an ordered pair.
That is:

A relation is a set R such that

$$(\forall u)\Big(u \in R \Longrightarrow (\exists a)(\exists b) u = (a,b)\Big) \tag{2.44}$$

2.1.1 How to think of a relation

You should picture an ordered pair as an arrow: the ordered pair (u, v) is represented by an arrow going from u to v.



The ordered pair (a, b).

And you should picture a relation as a set of arrows: for each u and each v, you draw an arrow from u to v to indicate that the pair (u, v) belongs to R.

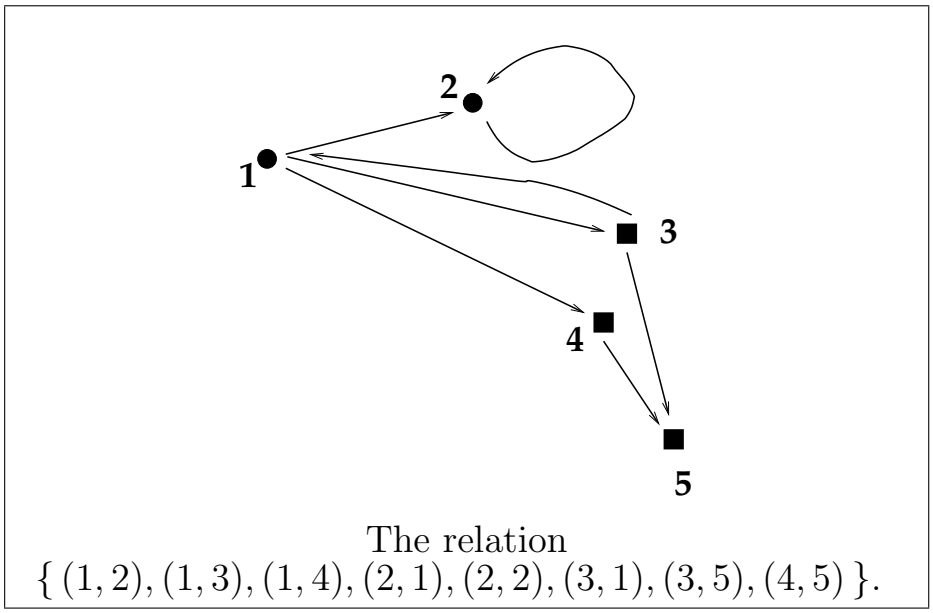
Another way to think of a relation R is as some kind of device that takes in "inputs" and produces "outputs". The pairs belonging to R are the ***input-output pairs*** produced by R.

Example 18. Consider the relation R given by

$$R = \{\,(1,2),(1,3),(1,4),(2,1),(2,2),(3,1),(3,5),(4,5)\,\}, \tag{2.45}$$

Then

- If you think of R as an input-output device, each pair in R gives you an input and a corresponding output, so that
  - the input 1 will produce the outputs 2, 3, and 4,
  - the input 2 will produce the outputs 1 and 2,
  - the input 3 will produce the outputs 1 and 5,
  - the input 4 will produce the output 5.
- If you think of R as a collection of arrows, here is R:



The relation
$\{ (1,2), (1,3), (1,4), (2,1), (2,2), (3,1), (3,5), (4,5) \}$.

2.1.2 Input, outputs, domain, range, source and target

Definition 18. If R is a relation, an input of R is an object x such that $(x, y) \in R$ for some y. □

(That is, x is an input of R if $(\exists y)(x, y) \in R$.)

Definition 19. If R is a relation, an output of R is an object y such that $(x, y) \in R$ for some x. □

(That is, y is an output of R if $(\exists x)(x, y) \in R$.)

Definition 20. If R is a relation and x is an input for R, an output of R for the input x is an object y such that $(x, y) \in R$.
(That is, y is an output of R for x if $(x, y) \in R$.) □

Definition 21. If R is a relation, the domain of R is the set of all inputs of R. We use $\mathrm{Dom}(R)$ to denote the domain of R. Therefore

$$\mathrm{Dom}(R) = \{x : (\exists y)(x, y) \in R\}. \tag{2.46}$$

Definition 22. If R is a relation, the range of R is the set of all outputs of R. We use $\mathrm{Ran}(R)$ to denote the range of R. Therefore

$$\mathrm{Ran}(R) = \{y : (\exists x)(x, y) \in R\}. \tag{2.47}$$

Definition 23. If R is a relation and S, T are sets, then

- we say that S is a source for R if every input of R belongs to S, i.e., if $\mathrm{Dom}(R) \subseteq S$,
- we say that T is a target for R if every output of R belongs to T, i.e., if $\mathrm{Ran}(R) \subseteq T$,
- we say that R is a relation from S to T if S is a spource for R and T is a target for R. □

Problem 14. ***Prove*** that if R is a relation and S, T are sets, then R is a relation from S to T if and only if $R \subseteq S \times T$. □

Definition 24. If R is a relation and A is a set, then we say that R is a relation on A if $R \subseteq A \times A$. □

It then follows from the result of Problem 14 that R is a relation on A if and only if $\mathrm{Dom}(R) \subseteq A$ and $\mathrm{Ran}(R) \subseteq A$.

Example 19. Let

$$R = \{\, (x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 = 1 \,\}. \tag{2.48}$$

Then

(I) R is a relation on $\mathbb{R}$,

(II) $\mathrm{Dom}(R) = [-1, 1]$, where

$$[-1, 1] = \{x \in \mathbb{R} : -1 \leq x \leq 1\}.$$

(III) $\mathrm{Ran}(R) = [-1, 1]$. □

2.2 Functions

2.2.1 An example of a function: the word "giraffe"

What kind of thing is the word "giraffe"? Since we are doing set theory here, and we would like to do everything using sets, we can ask, more precisely, ***what kind of set is the word "giraffe"?***.

A bad answer. The most obvious answer that one might think of is *the word 'giraffe' is a set of letters, namely, the 'seven member set'*

$$\{g, i, r, a, f, f, e\}.$$

This, however, cannot be right, for several reasons:

- The set $\{g, i, r, a, f, f, e\}$ is exactly the same as the set $\{g, i, r, a, f, e\}$. So this set is not a seven-member set at all. It is a six-member set. Just because I have written the letter "f" twice does not mean that the set "has f as a member twice", whatever that might possibly mean. A set is specified by specifying for each object x whether it is a member of the set or not. Whether I write that the letter "f" is a member of the set once, or twice, or three times, or 300 times, all this means is that "f" is a member of the set. (If I say ten times that Trump is the president, that doesn't make him "president ten times". All it means is that he is the president, and for some mysterious reason I have chosen to repeat that ten times.) So the set $\{g, i, r, a, f, f, e\}$ (that is, the set $\{g, i, r, a, f, e\}$), does not contain the information that in the word "giraffe" the letter "f" appears twice.

- The set $\{g, i, r, a, f, f, e\}$ (that is, the set $\{g, i, r, a, f, e\}$) is exactly the same as the sets $\{e, f, a, r, i, g\}$, $\{g, r, f, i, a, e\}$, or $\{f, a, r, i, g, e\}$. When I write the letters g, i, r, a, f, e, in that order, all that means is that the answer to the membership question "is x a member of the set?" is "yes" if x is the letter "g", or the letter "i", or the letter "r", or the letter "a", or the letter "f", or the letter "e", and the answer is "no" if x is anything else. It makes no difference whether I write this information in this particular order or not. So the set $\{g, i, r, a, f, f, e\}$ (that is, the set $\{g, i, r, a, f, e\}$), does not contain the information that in the word "giraffe" the letter "g" appears first, the letter "i" appears in the second place, the letter "r" appears in the third place, and so on.

The right answer. Now that we know that the word "giraffe" is not adequately represented by the set $\{g, i, r, a, f, f, e\}$, we can either

(a) give up on the idea of representing the word "giraffe" as a set,

or

(b) try to represent the word "giraffe" as a set in a more intelligent way.

Naturally, we choose (b). And we take advantage of the fact that we can use ***ordered pairs***. We represent the word "giraffe" as the following set:

$$\Big\{(1, g), (2, i), (3, r), (4, a), (5, f), (6, f), (7, e)\Big)\}\,. \tag{2.49}$$

This tells us that the first letter is a "g", the second letter is an "i", and so on.

Notice that it does not matter in which order we write the members of the set. For example, the sets

$$\Big\{(7, e), (6, f), (5, f), (4, a), (3, r), (2, i), (1, g)\Big\} \tag{2.50}$$

and

$$\Big\{(1, g), (3, r), (5, f), (6, f), (2, i), (4, a), (7, e))\Big\} \tag{2.51}$$

are exactly the same set as the one of (2.49). And they all give us exactly the same information: the first letter is "g", the second letter is "i", and so on.

The set (2.49), that we use to represent the word "giraffe", is a set of ordered pairs (x, y), where x is a natural number belonging to the set $\{1, 2, 3, 4, 5, 6, 7\}$, and y is a letter. So ***the set (2.49) is a relation***.

But there is more. ***the set (2.49) is a relation that has a very special additional property that not all relations have.***

To understand what that property is, ask yourself which word would be represented by the set

$$\Big\{(1, g), (2, i), (3, r), (4, a), (3, w), (5, f), (6, f), (7, e)\Big)\}\,. \tag{2.52}$$

Is it "giraffe" or "giwaffe"? You cannot tell, right? You cannot tell which letter occupies the third site, right? The set (2.52) tells us two contradictory

things: that the third letter is an "r" and that the third letter is a "w". So the set is "bad": we cannot use it to represent a word.

Why is the set (2.52) bad? The reason is that it contains the pairs $(3, r)$ and $(3, w)$. That is, ***the set (2.52) contains two pairs*** (x, y) ***with the same*** x ***but different*** y***'s***. This implies that we cannot tell which is the y that occupies site x.

- ***A relation that contains two pairs*** (x, y) ***with the same*** x ***but different*** y***'s is not a function.***
- ***A relation that does not contain two pairs*** (x, y) ***with the same*** x ***but different*** y***'s is a function.***
- ***The set (2.49) does not contain two pairs*** (x, y) ***with the same*** x ***but different*** y***'s. Therefore this set is a function.***
- ***The set (2.52) contains two pairs*** (x, y) ***with the same*** x ***but different*** y***'s. Therefore this set is not a function.***

Let us say the same thing in a slightly different way:

A function is a set f ***of ordered pairs, i.e., a relation, that has the following additional "unique output property":***

> ***(UOP) For each*** x***, there do not exist two different "values of the function at*** x***", i.e. there do not exist*** y, z ***such that*** $(x, y) \in f$***,*** $(x, z) \in f$***, and*** $y \neq z$***.***

Example 20. The set (2.49) is a function. The set (2.52) is not a function. □

Functions as input-output correspondences with the Unique Output Property. The property of the set (2.49) that makes is a function rather than a mere relation is Property (UOP). If you think of the function as representing a device, or rule, that for every "input" x produces an "output" y, the UOP says: ***if I specify an input, the function produces only one output for that input***.

2.2.2 The precise mathematical definition of "function"

Definition 25. A function is a relation f such that every input of f has the unique output property. □

That is,

A set f is a function if

(i) f is a set of ordered pairs.

(ii) for all x, y, z, if $(x, y) \in f$ and $(x, z) \in f$ then $y = z$.

In purely formal language,

A set f is a function if

(I) $(\forall u \in f)(\exists x)(\exists y)u = (x, y)$,

(II) $(\forall x)(\forall y)(\forall z)\Big(\big((x,y)\in f \wedge (x,z)\in f\big) \Longrightarrow y = z\Big)$.

2.2.3 The definition of "value" of a function at a member of its domain

Definition 26. If f is a function and $x \in \mathrm{Dom}(f)$ (that is, x is an input of f), then the value of f at x is the object $f(x)$ such that $f(x)$ is the unique output of f for x. (Recall that the definition of function tells us that every input of f has the unique output property, so the output for x is indeed unique.) □

2.2.4 The definition of "set where a function takes values"

Definition 27. If f is a function and V is a set, we say that f takes values in V, or that f is a function with values in V, or that f is a V-valued function, if $f(x) \in V$ for every $x \in \mathrm{Dom}(f)$. □

2.2.5 When are two functions equal?

The following theorem is the analogue for functions of the axiom on equality of sets: two sets are the same set if they have the same members. Here, the result says: two functions are the same function if they have the same domain and, for each member x of this domain, have the same values at x. And the result for functions is not an axiom; it's a ***theorem*** that we can ***prove***.

Theorem 8. *Let f, g be functions. Then $f = g$ if and only if* $\mathrm{Dom}(f) = \mathrm{Dom}(g)$ *and $f(x) = g(x)$ for every $x \in \mathrm{Dom}(f)$.*

Proof. It is clear that of $f = g$ then $\mathrm{Dom}(f) = \mathrm{Dom}(g)$ and $f(x) = g(x)$ for every $x \in \mathrm{Dom}(f)$. (*Proof:* Assume that $f = g$. We want to prove first that $\mathrm{Dom}(f) = \mathrm{Dom}(g)$. By the equality axiom, $(\forall u)u = u$. Specializing to $u = \mathrm{Dom}(f)$—using Rule $\forall_{use}$—we get $\mathrm{Dom}(f) = \mathrm{Dom}(f)$. Now, using SEE, since $f = g$, we can substitute "g" for the second f of "$\mathrm{Dom}(f) = \mathrm{Dom}(f)$" and get $\mathrm{Dom}(f) = \mathrm{Dom}(g)$. Now let us prove that $(\forall x \in \mathrm{Dom}(f))f(x) = g(x)$. Let x be an arbitrary member of $\mathrm{Dom}(f)$. Since $(\forall u)u = u$, we can use Rule $\forall_{use}$ and get $f(x) = f(x)$. Then, using SEE, since $f = g$, we can substitute "g" for the second f of "$f(x) = f(x)$" and get $f(x) = g(x)$. Since we have proved "$f(x) = g(x)$" for arbitrary x belonging to $\mathrm{Dom}(f)$, we can conclude that $(\forall x \in \mathrm{Dom}(f))f(x) = g(x)$.)

Now let us assume that $\mathrm{Dom}(f) = \mathrm{Dom}(g)$ and $f(x) = g(x)$ for every $x \in \mathrm{Dom}(f)$. We want to prove that $f = g$.

Since f and g are sets, it suffices to prove that $f \subseteq g$ and $g \subseteq f$. Both proofs are the same, so I will do only one of them.

Let us prove that $f \subseteq g$. Let u be an arbitrary member of f. Since f is a set of ordered pairs and $u \in f$, u is an ordered pair, so we may pick x, y such that $u = (x, y)$. Since $(x, y) \in f$, x is an input of f, so $x \in \mathrm{Dom}(f)$, and y is an output of f for x, so $y = f(x)$. Since $\mathrm{Dom}(f) = \mathrm{Dom}(g)$, and $x \in \mathrm{Dom}(f)$, we see that $x \in \mathrm{Dom}(g)$. Since $g(x) = f(x)$ and $y = f(x)$, it follows that $y = g(x)$. Then $(x, y) \in g$. So $u \in g$

So we have proved that every $u \in f$ is in g. Hence $f \subseteq g$.

As explained before, the proof that $g \subseteq f$ is identical, so we do omit it. **Q.E.D.**

2.2.6 The definition of "function mapping a set to a set"

Definition 28. If f, A, B are sets, we say that f is a function mapping A to B, and write

$$f : A \mapsto B\,,$$

if

1. f is a function,
2. A is the domain of f,
3. The range of f is a subset of B. □

In other words, "$f : A \mapsto B$" means "f is a function, A is the domain of f, and $f(x) \in B$ for every $x \in A$". Equivalently, "$f : A \mapsto B$" means "f is a function, A is the domain of F, and B is a target for f".

2.2.7 The "input-to-output" way to write names of functions

Let f be the integer part function that we have introduced before. We have seen how to describe this function

1. as a ***set of ordered pairs***:

$$f = \{(x, y) \in \mathbb{R}^2 : y \in \mathbb{Z} \wedge y \leq x \wedge y > x - 1\}\,. \tag{2.53}$$

2. by ***specifying the domain and giving a rule for computing*** $f(x)$ ***for each*** x ***in the domain***:

$$f(x) = \text{the largest } n \in \mathbb{Z} \text{ such that } n \leq x\,, \text{ for } x \in \mathbb{R}\,, \tag{2.54}$$

or

$$f(x) = [x] \quad \text{for } x \in \mathbb{R}\,. \tag{2.55}$$

There is a third way to write the name of a function, namely, the ***"input-to-output"*** way. This is a very convenient way to write functions, so we are going to use it a lot.

Here is how it goes, for the integer part function: we write

$$\text{the function } \mathbb{R} \ni x \mapsto [x]\,, \tag{2.56}$$

and read this as "the function that takes an x belonging to $\mathbb{R}$ and sends it (or "maps it") to the integer part of x".

If we want to indicate that the values are real numbers, we can also write

$$\text{the function } \mathbb{R} \ni x \mapsto [x] \in \mathbb{R}\,. \tag{2.57}$$

And if we want to stress that the values are actually integers, then we can write

$$\text{the function } \mathbb{R} \ni x \mapsto [x] \in \mathbb{Z}\,. \tag{2.58}$$

2.3 Examples of functions

2.3.1 The integer part function

The "integer part function" is the function f given by

$$f = \{(x, y) \in \mathbb{R}^2 : y \in \mathbb{Z} \wedge y \leq x \wedge y > x - 1\}\,. \tag{2.59}$$

It is easy to prove that

$$(\forall x \in \mathbb{R})(\exists! y \in \mathbb{Z})(y \leq x \wedge y > x - 1)\,. \tag{2.60}$$

(**I AM ASKING YOU TO PROVE THIS IN PROBLEM 15 BELOW.**)

If follows from (2.60) that

If f is the relation defined by (2.59, then

(IP1) f is a function,

(IP2) f satisfies

(*) ***If*** x ***is a real number, then*** $f(x)$ ***is the largest integer*** n ***such that*** $n \leq x$***.*** That is,

$$(\forall x \in \mathbb{R})\Big(f(x) \in \mathbb{Z} \wedge f(x) \leq x \wedge (\forall n \in \mathbb{Z})\Big(n \leq x \Longrightarrow n \leq f(x)\Big)\Big)\,. \tag{2.61}$$

Definition 29.

- The function f defined by (2.59) is called the integer part function.
- Instead of "$f(x)$", it is customary to write "$[x]$".
- And we read "$[x]$" as "the integer part of x". □

Example 21. Here are some values of the integer part function: $[9] = 9$, $[0] = 0$, $[6.2] = 6$, $[\pi] = 3$, $[-4.6] = -5$. □

Problem 15. ***Prove*** statement (2.60).

2.3.2 The "absolute value of a real number" function

The "absolute value of a real number function" is the function f given by

$$f = \{(x, y) \in \mathbb{R} \times \mathbb{R} : (x \geq 0 \wedge y = x) \vee (x \leq 0 \wedge y = -x)\}. \tag{2.62}$$

It is easy to prove that ***the set f defined by (2.62) is a function***. (**I AM ASKING YOU TO PROVE THIS IN PROBLEM 16 BELOW.**)

Definition 30.

- The function f defined by (2.62) is called the absolute value of a real number function.
- Instead of "$f(x)$", it is customary to write "$|x|$".
- And we read "$|x|$" as "the absolute value of x". □

We can also describe this function by specifying its domain and the rule for computing it, as follows:

Definition 31. The absolute value of a real number x is the real number $|x|$ given by

$$|x| = \begin{cases} x & \text{if} \quad x \geq 0 \\ -x & \text{if} \quad x \leq 0 \end{cases}. \tag{2.63}$$

And we can describe it in input-to-output notation by saying: "absolute value" is the function $\mathbb{R} \ni x \mapsto |x|$, where $|x|$ is given by (2.63)".

Example 22. Here are some values of the absolute value function: $|9| = 9$, $|-9| = 9$, $|0 = 0$, $|\pi| = \pi$, $|-\pi| = \pi$. □

2.3.3 Other "absolute value" functions

Naturally, we could also consider the "absolute value of a rational number" function f given by

$$f = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} : (x \geq 0 \Longrightarrow y = x) \wedge (x \geq 0 \Longrightarrow y = -x)\}, \quad (2.64)$$

and the "absolute value of an integer" function f given by

$$f = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : (x \geq 0 \Longrightarrow y = x) \wedge (x \geq 0 \Longrightarrow y = -x)\}, \quad (2.65)$$

These functions can also be described by specifying the domain and the rule for computing the function:

- The "absolute value of a rational number" function is the function f given by

$$f(x) = \begin{cases} x & \text{if} \quad x \geq 0 \\ -x & \text{if} \quad x \leq 0 \end{cases}, \qquad \text{for} \quad x \in \mathbb{Q}. \quad (2.66)$$

- The "absolute value of an integer" function is the function f given by

$$f(x) = \begin{cases} x & \text{if} \quad x \geq 0 \\ -x & \text{if} \quad x \leq 0 \end{cases}, \qquad \text{for} \quad x \in \mathbb{Z}. \quad (2.67)$$

And they can also be described with the "input-to-output" notation:

- The "absolute value of a rational number" function is the function $\mathbb{Q} \ni x \mapsto |x|$, where $|x| = x$ if $x \geq 0$ and $|x| = -x$ if $x \leq 9$,
- The "absolute value of an integer" function is the function $\mathbb{Z} \ni x \mapsto |x|$, where $|x| = x$ if $x \geq 0$ and $|x| = -x$ if $x \leq 9$,

Example 23. Here are some values of the absolute value function: $|9| = 9$, $|-9| = 9$, $|0 = 0$, $|\pi| = \pi$, $|-\pi| = \pi$. □

Problem 16.

1. ***Prove*** that the set f defined by

$$f = \{(x, y) \in \mathbb{R} \times \mathbb{R} : (x \geq 0 \wedge y = x + 1) \vee (x \leq 0 \wedge y = -x - 1)\} \quad (2.68)$$

is not a function. (***Give a precise, detailed proof.*** The main thing you have to do is prove for some real number x there exist two different real numberss y such that $(x, y) \in f$. That is, you have to find a real number x such that for two different real numbers y the sentence "$(x \geq 0 \Longrightarrow y = x + 1) \wedge (x \geq 0 \Longrightarrow y = -x - 1)$" is true.)

2. ***Prove*** that the set f defined by equation (2.62) is a function. (***Give a precise, detailed proof.*** The main thing you have to do is prove that for every real number x there exists a unique real number y such that the sentence "$(x \geq 0 \wedge y = x) \vee (x \geq 0 \wedge y = -x)$" is true.)

3. ***Determine*** the range of the function f defined by equation (2.62).

2.3.4 Squaring functions

We would like to define "the squaring function", that is, "the function f given by the formula $f(x) = x^2$". But, on order to define a function, we need to specify the domain, and if we do this in different ways we will get different functions, even if the formula $f(x) = x^2$ is the same.

The "square of a real number" function.
We define a function $f : \mathbb{R} \mapsto \mathbb{R}$ by letting

$$f(x) = x^2 \text{ for } x \in \mathbb{R}\,. \tag{2.69}$$

As a set of ordered pairs, f is given by

$$f = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y = x^2\}\,. \tag{2.70}$$

And in input-to-output notation, f is the function $\mathbb{R} \ni x \mapsto x^2$.

This is the "square of a real number" function. The domain of this function is the set $\mathbb{R}$ of all real numbers. The range is the set $\mathbb{R}_{\geq 0}$ of all nonnegative real numbers.

The "square of a rational number" function.
We define a function $f : \mathbb{Q} \mapsto \mathbb{Q}$ by letting

$$f(x) = x^2 \text{ for } x \in \mathbb{Q}\,. \tag{2.71}$$

As a set of ordered pairs, f is given by

$$f = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} : y = x^2\}\,. \tag{2.72}$$

And in input-to-output notation, f is the function $\mathbb{Q} \ni x \mapsto x^2$.

This is the "square of a rational number" function. The domain of this function is the set $\mathbb{Q}$ of all rational numbers. The range is the set of all nonnegative rational numbers whose square root is rational. (So, for example, 0, 1, 4, $\frac{4}{9}$ belong to the range of f, but -1, 2, 3, and $\frac{2}{3}$ do not.)

The "square of an integer" function.

We define a function $f : \mathbb{Z} \mapsto \mathbb{Z}$ by letting

$$f(x) = x^2 \text{ for } x \in \mathbb{Z}\,. \tag{2.73}$$

As a set of ordered pairs, f is given by

$$f = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : y = x^2\}\,. \tag{2.74}$$

In input-to-output notation, f is the function $\mathbb{Z} \ni x \mapsto x^2$.

This is the "square of an integer" function. The domain of this function is the set $\mathbb{Z}$ of all integers. The range is the set of all integers that are perfect squares. (An integer n is a perfect square if $n = m^2$ for some integer m.) (So, for example, 0, 1, 4, 9, 36, 121 belong to the range of f, but 2, 3, 7, 21, do not.)

The "Square of an integer modulo N functions"

If N is a natural number and $n \geq 2$, the integers modulo N, (also known as residues modulo N), are the integers $0, 1, 2, \ldots, N-1$. The set of all these residues modulo N is the denoted by $\mathbb{Z}_N$. So, for example:

$$\begin{aligned}
\mathbb{Z}_2 &= \{0, 1\}\,, \\
\mathbb{Z}_3 &= \{0, 1, 2\}\,, \\
\mathbb{Z}_4 &= \{0, 1, 2, 3\}\,, \\
&\vdots \quad\quad \vdots \\
\mathbb{Z}_{11} &= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}\,, \\
&\vdots \quad\quad \vdots \\
\mathbb{Z}_{243} &= \{n \in \mathbb{Z} : 0 \leq n < 243\}\,, \\
&\vdots \quad\quad \vdots
\end{aligned}$$

Each $\mathbb{Z}_N$ has an addition and multiplication operation, called $+_N$ and $\times_N$, which turn it into a commutative ring with identity.

Addition in $\mathbb{Z}_N$ is defined as follows: the sum $x +_N y$ of x and y in $\mathbb{Z}_N$ is the ordinary sum "reduced modulo N". (This means that $x +_N y$ is the remainder of dividing $x + y$ by N. For example: $5 +_{11} 8 = 2$, because $5 + 8 = 13$, and when we divide 13 by 11 we get a remainder of 2.) Similarly, the product $x \times_{11} y$ is the remainder of dividing $x \times y$ by N. For example:

$5 \times_{11} 8 = 7$, because $5 \times 8 = 140$ and when we divide 40 by 11 we get a remainder of 7.

It follows that we can talk, in $\mathbb{Z}_N$, about the "square" of a member x of $\mathbb{Z}_N$. The square of a member x of $\mathbb{Z}_N$ is the member x^2 of $\mathbb{Z}_N$ given by $x^2 = x \times_N x$.

And then we can consider the "squaring in $\mathbb{Z}_N$" function. Let us call this function Sq_N. Then Sq_N is the set of ordered pairs

$$Sq_N = \{(x, y) \in \mathbb{Z}_N \times \mathbb{Z}_N : y = x^2\}\,. \tag{2.75}$$

And we can describe it as a rule

$$Sq_N(x) = x^2 \quad \text{for } x \in \mathbb{Z}_N\,. \tag{2.76}$$

Or, in input-to-output notion, as

$$Sq_N \text{ is the function } \mathbb{Z}_N \ni x \mapsto x^2 \in \mathbb{Z}_N\,. \tag{2.77}$$

The domain of Sq_N is $\mathbb{Z}_N$.

A very interesting a very important question is ***"how many members does the range of*** Sq_N ***have?"***. We will have a lot to say about that issue later. But here I will just give you a few examples:

1. The range of Sq_7 is the set $\{0, 1, 2, 4\}$, because in $\mathbb{Z}_7$ the following are true: $0^2 = 0$, $1^2 = 1$, $2^2 - 4$, $3^2 = 2$, $4^2 = 2$, $5^2 = 4$, and $6^2 = 1$, so the members of $\mathbb{Z}_7$ that are squares are 0, 1, 2 and 4.

2. The range of Sq_8 is the set $\{0, 1, 4\}$, because in $\mathbb{Z}_8$ the following are true: $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 1$, $4^2 = 0$, $5^2 = 1$, $6^2 = 4$, and $7^2 = 1$, so the members of $\mathbb{Z}_8$ that are squares are 0, 1, and 4.

3. The range of Sq_{11} is the set $\{0, 1, 3, 4, 5, 9\}$, because in $\mathbb{Z}_{11}$ the following are true: $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 5$, $5^2 = 3$, $6^2 = 3$, $7^2 = 5$, $8^2 = 9$, $9^2 = 4$, and $10^2 = 1$, so so the members of $\mathbb{Z}_{11}$ that are squares are 0, 1, 3, 4, 5, and 9.

2.3.5 Functions of two variables

Definition 32. A function of two variables is a function whose domain is a set of ordered pairs. □

Example 24. Let f be the function

$$\mathbb{R} \times \mathbb{R} \ni (x, y) \mapsto 3x - 2y \in \mathbb{R}\,. \tag{2.78}$$

This function takes as input a pair (x, y) of real numbers, and produces as output the real number $3x - 2y$.

Remark 6. If we wanted to write the function (2.78) using the familiar "$f(x)$" notation, we would have to write "$f\Big((x, y)\Big) = 3x - 2y$". However, ***it is customary to omit one of the pairs of parentheses, and just write*** "$f(x, y) = 3x - 2y$". □

The function (2.78) can be described as a set of ordered pairs:

$$f = \Big\{\, \big((x, y), z\big) \in (\mathbb{R} \times \mathbb{R}) \times \mathbb{R} : z = 3x - 2y \,\Big\}\,.$$

Notice that f ***is a set of ordered pairs*** (u, v) ***for which*** u ***itself is an ordered pair***. The expression "$((x, y), z)$" stands for "the ordered pair of the ordered pair (x, y) and the real number z".

One can also write the function (2.78) by specifying the domain and the rule for computing the function, that is, by writing

$$f(x, y) = 3x - 2y \qquad \text{for } (x, y) \in \mathbb{R} \times \mathbb{R}\,. \tag{2.79}$$

Example 25. ***The operations of addition, subtraction, multiplication and division of real numbers are functions of two variables.***

For example,

- addition of real numbers is the function

  $$\mathbb{R} \times \mathbb{R} \ni (x, y) \mapsto x + y \in \mathbb{R}\,,$$

  that is, the set

  $$\Big\{\, \big((x, y), z\big) \in (\mathbb{R} \times \mathbb{R}) \times \mathbb{R} : z = x + y \,\Big\}\,;$$

- subtraction of real numbers is the function

  $$\mathbb{R} \times \mathbb{R} \ni (x, y) \mapsto x - y \in \mathbb{R}\,,$$

  that is, the set

  $$\Big\{\, \big((x, y), z\big) \in (\mathbb{R} \times \mathbb{R}) \times \mathbb{R} : z = x - y \,\Big\}\,;$$

- multiplication of real numbers is the function

$$\mathbb{R} \times \mathbb{R} \ni (x, y) \mapsto x.y \in \mathbb{R}\,,$$

that is, the set

$$\left\{ \big((x, y), z\big) \in (\mathbb{R} \times \mathbb{R}) \times \mathbb{R} : z = x.y \right\};$$

- division of real numbers is the function

$$\mathbb{R} \times (\mathbb{R} - \{0\}) \ni (x, y) \mapsto x.y \in \mathbb{R}\,,$$

that is, the set

$$\left\{ \big((x, y), z\big) \in (\mathbb{R} \times (\mathbb{R} - \{0\}) \times \mathbb{R} : y \neq 0 \wedge y.z = x \right\},$$

where $\mathbb{R} - \{0\}$ ("$\mathbb{R}$ with zero removed") is the set $\{x \in \mathbb{R} : x \neq 0\}$.

Remark 7. In the formulas involving the division function, we have had to restrict the values of y by requiring that $y \neq 0$. That is, ***the domain of the division function is not*** $\mathbb{R} \times \mathbb{R}$***, the set of all pairs*** (x, y) ***of real numbers, but only*** $\mathbb{R} \times (\mathbb{R} - \{0\})$***, the set of all pairs*** (x, y) ***of real numbers for which*** $y \neq 0$***.***

The reason for that is that, as you know very well, it is not possible to divide by zero. So the function $(x, y) \mapsto \frac{x}{y}$, i.e. the function that takes a pair (x, y) and produces $\frac{x}{y}$ as its output, cannot admit a pair of the form $(x, 0)$ as an input. □

2.3.6 Binary operations as functions

A "binary operation" on a set S is, roughly, a "rule" (whatever that means) that for every two members x, y of the set produces a third member z, called "the result of applying the operation to x and y".

The precise meaning of this should now be clear.

Definition 33. A binary operation on a set S is a function $f : \mathrm{Dom}(f) \mapsto S$ whose domain $\mathrm{Dom}(f)$ is a subset of $S \times S$.

The binary operation f is everywhere defined on S if $\mathrm{Dom}(f) = S \times S$.

The binary operation f is partially defined on S if $\mathrm{Dom}(f) \neq S \times S$. □

Example 26.

- Addition, subtraction and multiplication of real numbers are everywhere defined binary operations on $\mathbb{R}$.
- Division of real numbers is a partially defined binary operation on $\mathbb{R}$.
- Addition, subtraction and multiplication of integers are everywhere defined binary operations on $\mathbb{Z}$.
- Division of integers is a partially defined binary operation on $\mathbb{Z}$. □
- Addition and multiplication of natural numbers are everywhere defined binary operations on $\mathbb{N}$.
- Subtraction and division of natural numbers are partially defined binary operations on $\mathbb{N}$. □

Problem 17.

1. ***Write down*** the definitions of the operations of addition, subtraction, multiplication and division on the set $\mathbb{N}$ of natural numbers (a) as sets of ordered pairs, (b) as rules specifying the domain and how to compute the function, and (c) as input-to-output descriptions.
2. ***Prove*** that subtraction and division of natural numbers are partially defined operations and ***describe precisely*** the domains of each of the operations. □

How we write operations: the infix notation. As you well know, if f is the addition of real numbers operation, we do not write "$f(x, y)$" for the value of this function at (x, y); we write "$x + y$", which means two things:

- we don't use the symbol 'f"; we use he symbol "+" instead,
- we put the symbol in the middle, not before the pair (x, y).

A symbol or string of symbols that is added to word by putting it in the middle of a word is called an infix. In English, it is very common to use ***prefixes*** and ***suffixes***. (A prefix is a symbol or string if symbols added at the beginning of a word, such as, for example, "re" in "recover" or "reheat", or "up" in "upbringing". A suffix is a symbol or string if symbols added at

the end of a word, such as, for example, "ing" in "carrying" or "pushing".) Even though prefixes and suffixes are very common in English, infixes are extremely rare, but they do occur. (Example: the "*s*" in "passersby".)

In Mathematics, infixes are used all the time. In particular, many binary operations are written as infixes. For example:

- For addition, we use the symbol "+" and infix notation, and write "$x + y$" rather than either (a) calling the operation "f" and writing "$f(x, y)$", or (b) calling the operation "+" and writing "$+(x, y)$".
- For subtraction, we use the symbol "$-$" and infix notation, and write "$x - y$".
- For multiplication, we use the symbols "$\times$" and "$\cdot$", and write "$x \times y$", or "$x \cdot y$". And sometimes we just write[9] "xy".
- For division, the symbol "$\div$" is used sometimes, in infix notation, so we write "$x \div y$". But, as you well know, it is much more common to write "$\frac{x}{y}$".

Problem 18. Define a binary operation "$\uparrow$" on $\mathbb{R}$ by letting

$$x \uparrow y = \begin{cases} x & \text{if} \quad x \geq y\,, \\ y & \text{if} \quad y \geq x\,. \end{cases} \tag{2.80}$$

Then $x \uparrow y$ is the larger of x and y.

1. ***Write*** a description of $\uparrow$ as a set of ordered [airs.
2. ***Prove*** that the operation "$\uparrow$" satisfies the *commutative law*

$$(\forall x \in \mathbb{R})(\forall y \in \mathbb{R}) x \uparrow y = y \uparrow x\,, \tag{2.81}$$

and the *associative law*

$$(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R}) x \uparrow (y \uparrow z) = (x \uparrow y) \uparrow z\,. \tag{2.82}$$

3. ***Prove*** that the operations "$\uparrow$" and "+" satisfy the *distributive law of addition with respect to* $\uparrow$:

$$(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R}) x + (y \uparrow z) = (x + y) \uparrow (x + z)\,. \tag{2.83}$$

[9] How shall I call this? "Zerofix"? "Nofix"? "Nothingfix"?

4. ***Prove or disprove*** that the operations "↑" and "+" satisfy the *distributive law of ↑ with respecto to addition*:

$$(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R}) x \uparrow (y+z) = (x+y) \uparrow (x+z)\,. \quad (2.84)$$

5. ***Prove*** that

$$(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})\ x \uparrow y = \frac{x+y+|x-y|}{2}\,. \quad (2.85)$$

2.4 Composition of functions

Definition 34. If A, B, C are sets, $f : A \mapsto B$ and $g : B \mapsto C$, the composite function of f and g is the function $g \circ f : A \mapsto C$ given by

$$g \circ f(x) = g\big(f(x)\big) \qquad \text{for every} \quad x \in A\,.$$

The following theorem says that the operation of composition of functions satisfies the associative law in the sense that when both $h \circ (g \circ f)$ and $(h \circ g) \circ f$ are defined, they are equal

Theorem 9. *Let A, B, C, D be sets, and assume that $f : A \mapsto B$, $g : B \mapsto C$, and $h : C \mapsto D$. Then*

$$h \circ (g \circ f) = (h \circ g) \circ f\,. \quad (2.86)$$

Proof. **YOU DO IT.**

Problem 19. ***Prove*** Theorem 9. □

2.4.1 The definition of "one-to-one function"

Definition 35. A function f is one-to-one (or injective) if whenever two inputs are different, the values of f at those inputs are different as well.

In other words: f is one-to-one if

$$(\forall u \in \mathrm{Dom}(f))(\forall v \in \mathrm{Dom}(f))(u \neq v \Longrightarrow f(u) \neq f(v))\,. \quad (2.87)$$

Equivalently, f is one-to-one if

$$(\forall u \in \mathrm{Dom}(f))(\forall v \in \mathrm{Dom}(f))\big(f(u) = f(v) \Longrightarrow u = v\big)\,. \quad (2.88)$$

2.4.2 The composite of two one-to-one functions

Theorem 10. *Let A, B, C be sets, and assume that $f : A \mapsto B$, $g : B \mapsto C$, and both f and g are one-to-one. Then $g \circ f$ is one-to-one.*

Proof. Let $h = g \circ f$. We want to prove that h is one-to-one.

For that purpose, we prove that if $x_1 \in A$, $x_2 \in A$, and $x_1 \neq x_2$, it follows that $h(x_1) \neq h(x_2)$.

Let $y_1 = f(x_1)$, $y_2 = f(x_2)$, Since f is one-to-one and $x_1 \neq x_2$, we can conclude that $y_1 \neq y_2$.

Then, since g is one-to-one and $y_1 \neq y_2$, we can conclude that $g(y_1) \neq g(y_2)$.

But $g(y_1) = g(f(x_1)) = h(x_1)$, and $g(y_2) = g(f(x_2)) = h(x_12)$. So $h(x_1) \neq h(x_2)$, as desired. **Q.E.D.**

2.4.3 The definition of "function onto a set"

Definition 36. A function $f : A \mapsto B$ is <u>onto B</u> if $B = \mathrm{Ran}(f)$.

In other words, f is onto B if

$$(\forall b \in B)(\exists a \in A) f(a) = b\,. \tag{2.89}$$

Example 27. Let f be the "squaring a real number" function.

The domain $\mathrm{Dom}(f)$ is $\mathbb{R}$, the set of all real numbers. And, for $x \in \mathbb{R}$, the value $f(x)$ is given by

$$f(x) = x^2\,.$$

Then the range $\mathrm{Ran}(f)$ is $\mathbb{R}_{\geq 0}$, the set of all nonnegative real numbers. (Reason: every nonnegative real number has a square root.)

Then both statements "$f : \mathbb{R} \mapsto \mathbb{R}$" and "$f : \mathbb{R} \mapsto \mathbb{R}_{\geq 0}$" are true. And f is onto $\mathbb{R}_{\geq 0}$ but f is not onto $\mathbb{R}$. □

Remark 8. The previous example shows that ***the sentence "f is onto" is meaningless***, in the same way as the the sentence "a is divisible" is meaningless.

There is no such thing as "being divisible". What makes sense is "being divisible by some number". "Divisible" is a 2-argument predicate: we say things like "a is divisible by b", and we do not say things like "a is divisible". Similarly, "is onto" is a 2-argument predicate: we say things like "f is onto B", and we do not say things like "f is onto". □

2.4.4 The composite of two onto functions

Theorem 11. *Let A, B, C be sets, and assume that $f : A \mapsto B$, $g : B \mapsto C$, f is onto B and g is onto C. Then $g \circ f$ is onto C.*

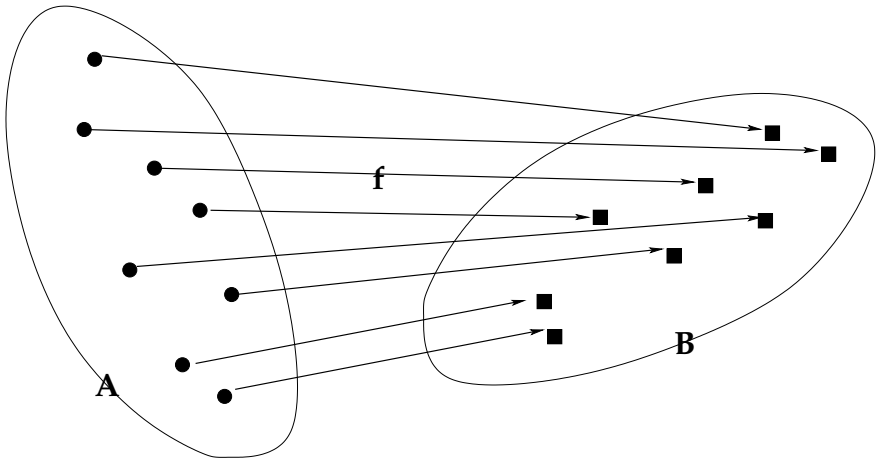
Proof. **YOU DO IT.**

Problem 20. ***Prove*** Theorem 11. □

2.5 The definition of "bijection"

Definition 37. A function $f : A \mapsto B$ is a bijection from A to B if it is one-to-one and onto B.

In other words, ***a function*** $f : A \mapsto B$ ***is a bijection from*** A ***to*** B ***if*** f ***is one-to-one and*** $\mathrm{Ran}(f) = B$. □



A bijection

We can tell that A (the set of circles) and B (the set of squares) have the same number of members because f (the set of arrows, i.e. of ordered pairs) is a bijection from A to B:

- the arrows send every circle to one and only one square (that is, f is a function),
- different circles are sent to different squares (that is, f is one-to-one),
- no square is left out (that is, f is onto).

Theorem 12. *The empty set is a bijection from the empty set to the empty set.*

Proof. **YOU PROVE THIS.**

Problem 21. ***Prove*** Theorem 12.

You have to prove several things:

1. that $\emptyset$ is a relation, i.e., a set of ordered pairs. (So you have to prove that every member of $\emptyset$ is an ordered pair.)
2. that $\emptyset$ is in fact a function. (So you have to prove that

$$(\forall x)(\forall y)(\forall z)\Big(\big((x,y)\in\emptyset\wedge(x,z)\in\emptyset\big)\Longrightarrow y=z\Big),$$

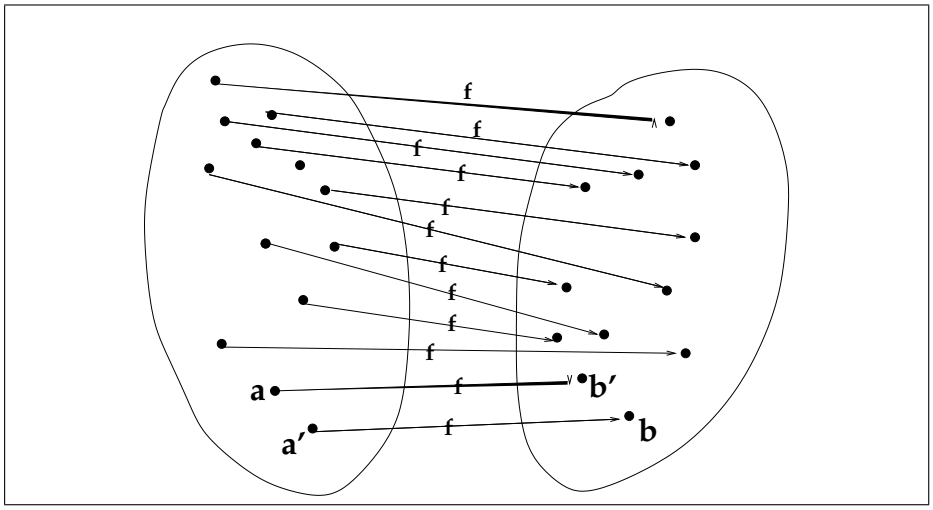
3. that the domain of $\emptyset$ is $\emptyset$,
4. that $\emptyset : \emptyset \mapsto \emptyset$,
5. that $\emptyset$ is one-to-one,
6. that $\emptyset$ is onto $\emptyset$. □

2.5.1 The exchange lemma

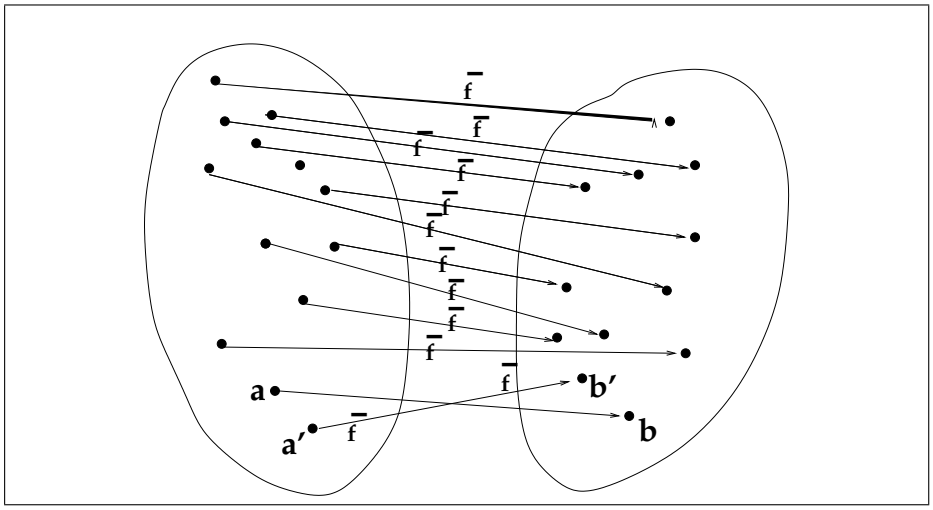
The following theorem is rather simple, but very important. To understand what it says, think of of an example. Suppose you have several couples dancing in a large ballroom: every man is dancing with one and only one woman, every woman is danving with one and only one man. That means that we have in front of our eyes a bijection f from M to W, where M is the set of all the men that are dancing, and W is the set of all the women. The bijection $f : M \mapsto W$ is defined as follows: for $m \in M$, $f(m)$ is the woman with whom m is dancing.

Theorem 13 then says that, if we are interested in a particular man a and a particular woman b, we can rearrange things so that a will be dancing with b. And the way we do that is as follows: if a is already dancing with b then we do not have to do anything. And if a is not dancing with b, that means that a is dancing with some other woman b', and b is dancing with some other man a'. So in this case we just have the two couples (a, b'), (a', b) ***exchange partners***: we remove the pairs[10] (a, b'), (a', b) from f and put, instead, the pairs (a, b) and (a', b'), this gives rise ot a new bijection $\bar{f}$. And $\bar{(a)}$ is b, as we wanted.

[10]Do not forget that f is a set of ordered pairs. The fact that a is dancing with b' and a' is dancing with b means that $b' = f(a)$ and $b = f(a')$, and this in turn means that the pairs (a, b') and (a', b) are members of f.



The bijection f sends a to b', but we want a bijection $\bar{f}$ that sends a to b. We construct $\bar{f}$ by finding a' such that $f(a') = b$, and having a and a' "trade parners": $\bar{f}$ sends a to b, and a' to b'. The partners of the other members of $\mathrm{Dom}(f)$ are not changed.



Theorem 13. *Suppose A, B are sets, $f : A \mapsto B$, and f is a bijection from A to B. Then for every $a \in A$ and every $b \in B$ there exists a bijection $\bar{f}$ from A to B such that $\bar{f}(a) = b$.*

Proof. **YOU PROVE THIS.**

Problem 22. ***Prove*** Theorem 13. Make sure you write a complete, detailed proof of the fact that the function $\bar{f}$ that you define is a bijection.

HINT: Read carefully the explanation before the statement of the theorem, and look at the pictures. All you have to do is repeat the same construction of $\bar{f}$ in general, for any sets A, B, and bijection f, without mentioning "men", "women", and "dancing". □

2.5.2 The composite of two bijections

Theorem 14. *Let A, B, C be sets, and assume that f is a bijection from A to B and g is a bijection from B to C. Then the composite function $g \circ f$ is a bijection from A to C.*

Proof. Let $h = g \circ f$. We want to prove that h is a bijection.

Since f and g are bijections, they are one-to-one. Hence h is one-to-one by Theorem 10.

Since f and g are bijections, f is onto B and g is onto C. Hence h is onto C by Theorem 11.

So h is one-to-one and onto C. Therefore h is a bijection from A to C. **Q.E.D.**

2.5.3 The identity function of a set

Definition 38. If A is a set, the identity function of A, or identity map of A, is the function $1_A : A \mapsto A$ such that

$$1_A(x) = x \qquad \text{for every } x \in A\,. \tag{2.90}$$

The reason 1_A is called the "identity function" is that it behaves, with respect to the operation of function composition, very much like the number 1 behaves with respect to the operation of multiplication of numbers:

- Multiplying a number by 1 yields the same number: $x \cdot 1 = x$ for every number x.
- Composing a function with 1_A yields the same function, except only for the detail that now we have to be careful about domains: $f \circ 1_A$ makes sense for functions $f : A \mapsto B$ (for any B), whereas $1_A \circ f$ makes sense for functions $f : B \mapsto A$ (for any B). The precise result is Theorem 15 below.

Theorem 15. *If A, B are sets, then*

$$f \circ 1_A = f \qquad \text{if} \qquad f : A \mapsto B\,, \tag{2.91}$$

$$1_A \circ f = f \qquad \text{if} \qquad f : B \mapsto A\,. \tag{2.92}$$

Proof. Suppose $f : A \mapsto B$. Since $1_A : A \mapsto A$, it follows that $f \circ 1_A : A \mapsto B$. So both f and $f \circ 1_A$ have domain A.

To prove that the functions $f \circ 1_A$ and f are equal it suffices, according to Theorem 8, to prove that they have the same domain and that they have the same value for every x in that domain.

We already know that $f \circ 1_A$ and f have the same domain, because both have domain A. If $x \in A$, then

$$(f \circ 1_A)(x) = f(1_A(x)) = f(x)\,,$$

So $(f \circ 1_A)(x) = f(x)$. This completes the proof that $\boxed{f \circ 1_A = f}$.

Now let us suppose that $f : B \mapsto A$. Since $1_A : A \mapsto A$, it follows that $1_A \circ f : B \mapsto A$. So both f and $1_A \circ f$ have domain B.

To prove that the functions $1_A \circ f$ and f are equal it suffices, according to Theorem 8, to prove that they have the same domain and that they have the same value for every x in that domain.

We already know that $1_A \circ f$ and f have the same domain, because both have domain B. If $x \in B$, then

$$(1_A \circ f)(x) = 1_A(f(x)) = f(x)\,,$$

So $(1_A \circ f)(x) = f(x)$, and this completes the proof that $\boxed{1_A \circ f = f}$.**Q.E.D.**

Theorem 16. *If A is a set, then 1_A is a bijection from A to A.*

Proof. **YOU DO IT.**

Problem 23. ***Prove*** Theorem 16. □

2.5.4 The inverse of a relation

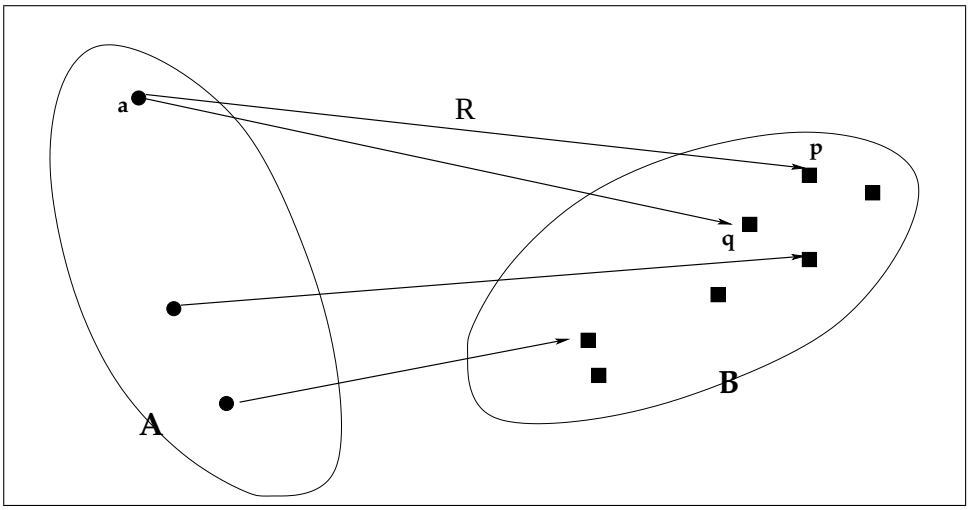
If you think of a relation R as a set of arrows (or of ordered pairs, which amounts to the same thing), then it is clear that can define another relation R^1 by just reversing the arrows of R: for every arrow of R going from a point x to a point y, we put in R^{-1} an arrow going from y to x. (Or, in terms of ordered pairs: R^{-1} consists of all the pairs (u, v) such that $(v, u) \in R$.)

Definition 39. If R is a relation, then the inverse of R is the relation R^{-1} given by

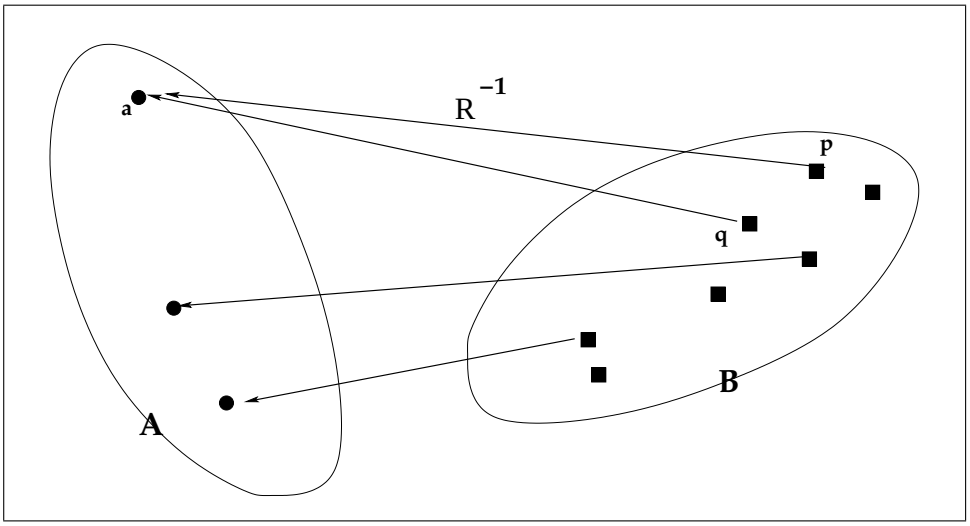
$$R^{-1} = \{(u, v) : (v.u) \in R\}\,. \tag{2.93}$$

Now that we know what the inverse of a relation is, it is clear that various properties of R correspond to properties of R^{-1}.

For example, consider the following relation (i.e., set of ordered pairs, or set of arrows) R:



and its inverse R^{-1}:



We see that R ***is not a function***, because there is one point a which is the source of two different arrows ending at two different points p, q. (So R violates the unique output property: the input u gives rise to two different outputs, p and q.)

What does this tell us about R^{-1}? It tells us that R^{-1} is not one-to-one, because there are two different squares (i.e, inputs for R^{-1}) that are sources of arrows going to the same point. (Reason: both p and q are sent by R^{-1} to the same point a.)

This tells us that if R is a function then R^{-1} should be one-to-one, and if R is one-to-one then R^{-1} should be a function. In particular, we have:

Theorem 17. *If f is a function, then*

- *the relation f^{-1} is a function if and only if f is one-to-one,*
- *if f is one-to-one, then the domain of f^{-1} is the range of f.*

Proof. **YOU DO THIS.**

Problem 24. ***Prove*** Theorem 17. □

2.5.5 The inverse of the inverse

Theorem 18. *If R is a relation, then the inverse of the inverse of R is R. That is,*

$$R = \left(R^{-1}\right)^{-1}.$$

Proof. **YOU DO THIS.**

2.5.6 The inverse of a bijection

Theorem 19. *If A, B are sets, and f is a bijection from A to B, then f^{-1} is a bijection from B to A.*

Proof. We use Theorem 17 repeatedly.

Since f is a bijection, f is one-to-one, so by Theorem 17, f^{-1} is a function. Since the inverse of f^{-1} is f, and f is a function it follows from Theorem 17 that f^{-1} is one-to-one.

Since f is a function from A onto B, the range of f is B, so by Theorem 17 the domain of f^{-1} is B.

Since f^{-1} is a one-to-one, Theorem 17 tells that the domain of $(f^{-1})^{-1}$ is the range of f^1. But $(f^{-1})^{-1} = f$, so the domain of F is the range of f^{-1}. But the domain of f is A, so the range of f^{-1} is A, which menas that f^{-1} is a function onto A.

So $f^{-1} : B \mapsto A$, f^{-1} is one-to-one, and f^{-1} is onto A. So f^{-1} is a bijection from B to A. **Q.E.D.**

2.5.7 Some problems

Problem 25. ***Prove*** Theorem 18.

HINT: This is trivial. The proof should be no more than one or two lines. □

Problem 26. ***Prove*** that if $f : A \mapsto B$, then f is a bijection from A to B if and only if the following is true:

(#) There exists a function $g : B \mapsto A$ such that $g \circ f = 1_A$ and $f \circ g = 1_B$.

(The meaning of the notation "1_A" is explained in section 2.5.3.) □

Problem 27. For each of the following relations R:

1. ***Find*** the domain and the range of R, and ***give rigorous proofs*** of your assertions;
2. ***determine*** whether R is a function and ***prove*** your answer;
3. if R is a function, ***express*** R in "input-to-output" notation, as explained in section 2.2.7. (For example, if R was the function $\{(x, y) \in \mathbb{Z}\times\mathbb{Z} : y = x^2+3\}$, you would write "$R$ is the function $\mathbb{Z} \ni x \mapsto x^2+3$".)
4. if R is a function, ***determine*** whether it is one-to-one or not and ***prove*** your answer.
5. If R is a function, ***give examples*** of
   (a) a set B such that $R : \mathrm{Dom}(f) \mapsto B$ and R is onto B.
   (b) a set C such that $R : \mathrm{Dom}(f) \mapsto C$ but R is not onto C.

$$
\begin{aligned}
R &= \{(x,y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 = 1\}, && (2.94)\\
R &= \{(x,y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 = 1 \wedge y > 0\}, && (2.95)\\
R &= \{(x,y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 = 1 \wedge y \geq 0\}, && (2.96)\\
R &= \{(x,y) \in \mathbb{R} \times \mathbb{R} : xy = 1\}, && (2.97)\\
R &= \left\{(x,y) \in \mathbb{R} \times \mathbb{R} : y = \frac{1}{1+x^2}\right\}, && (2.98)\\
R &= \{(x,y) \in \mathbb{R} \times \mathbb{R} : x^3 + y^3 = 2\}, && (2.99)\\
R &= \left\{(x,y) \in \mathbb{R} \times \mathbb{R} : y = \frac{x}{1+x^2}\right\}, && (2.100)\\
R &= \{(x,y) \in \mathbb{Z} \times \mathbb{R} : 2^x y = 1\}, && (2.101)\\
R &= \{(x,y) \in \mathbb{N} \times \mathbb{R} : 2^x y = 1\}. && (2.102)
\end{aligned}
$$

Problem 28. ***Prove or disprove*** each of the following statements. (NOTE; two of the statetents are true; the other four are false.)

1. If A, B, C are sets, $f : A \mapsto B$ and $g : B \mapsto C$ are functions, and $g \circ f$ is one-to-one, then f is one-to-one.

2. If A, B, C are sets, $f : A \mapsto B$ and $g : B \mapsto C$ are functions, and $g \circ f$ is one-to-one, then g is one-to-one.

3. If A, B, C are sets, $f : A \mapsto B$ and $g : B \mapsto C$ are functions, and $g \circ f$ is onto C then f is onto B.

4. If A, B, C are sets, $f : A \mapsto B$ and $g : B \mapsto C$ are functions, and $g \circ f$ is onto C, then g is onto to C.

5. If A, B, C are sets, $f : A \mapsto B$ and $g : B \mapsto C$ are functions, and $g \circ f$ is a bijection from A to C, then g is a bijection from B to C.

6. If A, B, C are sets, $f : A \mapsto B$ and $g : B \mapsto C$ are functions, and $g \circ f$ is a bijection from A to C, then f is a bijection from A to B.

3 Finite sets

3.1 An important notational convention: the sets $\mathbb{N}_k$

In what follows we will be making lots of statements about "the natural numbers $1, 2, \ldots, k$", that is "all the natural numbers j such that $j \leq k$". So it will be convenient to give a name to the set of all such js.

THE SETS $\mathbb{N}_k$ (A.K.A. $\{1, 2, \ldots, k\}$)

The expression "$\mathbb{N}_k$" stands for the set of all natural numbers that are less than or equal to k. That is,

$$\mathbb{N}_k = \{n \in \mathbb{N} : n \leq k\}. \tag{3.103}$$

Another notation often used for this set is "$\{1, \ldots, k\}$", or "$\{1, 2, \ldots, k\}$". We will use "$\mathbb{N}_k$" when k is a natural number, and also when $k = 0$. (So $\mathbb{N}_k$ makes sense when $k \in \mathbb{N} \cup \{0\}$.)
Naturally, for $n = 0$ the set defined by (3.103) has no members, because there are no natural numbers k such that $k \leq 0$. So $\mathbb{N}_0 = \emptyset$.
Here are other examples:

$$\mathbb{N}_1 = \{1\}, \quad \mathbb{N}_2 = \{1, 2\}, \quad \mathbb{N}_3 = \{1, 2, 3\},$$
$$\mathbb{N}_4 = \{1, 2, 3, 4\}, \quad \mathbb{N}_5 = \{1, 2, 3, 4, 5\}, \quad \mathbb{N}_6 = \{1, 2, 3, 4, 5, 6\},$$

Then

$$j \in \mathbb{N}_k$$
is just another way of saying "$j \in \mathbb{N}$ and $j \leq k$".

3.2 Finite lists (a.k.a. finite sequences, or n-tuples)

Definition 40. If $n \in \mathbb{N} \cup \{0\}$ (i.e., if n is a nonnegative integer), then a function whose domain is the set $\mathbb{N}_n$ is called a finite list of length n, or a finite sequence of length n, or an n-tuple. □

Example 28. The set L given by

$$L = \{(1,2),(2,3),(3,5),(4,7)\}$$

is is a finite list of length 4, because

- L is a set of ordered pairs, so L is a relation,
- L has the unique output property, so L is a function,
- the domain of L is the set $\mathbb{N}_4$, so L is a list of length 4. □

3.2.1 The entries of a list: entries vs. members

Definition 41. If f is a finite list of length n and $j \in \mathbb{N}_n$, then $f(j)$ is the j-th entry of the list. □

Lists have ***entries***, not members.
Sets have ***members***, not entries.

Example 29. We saw in Example 28 that the set L given by

$$L = \{(1,2),(2,3),(3,5),(4,7)\}$$

is is a finite list of length 4.

The name of this list, written in a way that shows that it is a list, is

$$(2,3,5,7)\,.$$

So we can say things like "The list of the first four prime numbers is $(2,3,5,7)$."

We can also write this in ***dummy variable notation***, and call the list

$$(p_j)_{j=1}^{4},\ \text{where, for each } j \in \mathbb{N}_4\,,\ p_j \text{ is the } j-\text{th prime number}\,.$$

Example 30. The word "giraffe" is a list of seven letters: (g,i,r,a,f,f,e).

As we say in section 2.2.1, on page 58, this list is a function, namely, the set of ordered pairs

$$\text{“}giraffe'' = \Big\{(1,g),(2,i),(3,r),(4,a),(5,f),(6,f),(7,e)\Big)\}\,. \qquad (3.104)$$

This means that:

- the first entry is "g",
- the second entry is "i",
- the third entry is "r",
- the fourth entry is "a",
- the fifth entry is "f",
- the sixth entry is "f",
- the seventh entry is "e".

The domain of this list is $\mathbb{N}_7$, and the range is the set $\{g, i, r, a, f, e\}$. That is,

$$\text{Ran}(\text{“giraffe”}) = \{g, i, r, a, f, e\}. \tag{3.105}$$

Notice that the list (i.e. function) "giraffe" has seven entries, but the set $\text{Ran}(\text{“}giraffe\text{”})$ has six members.

Notice also that the function "$giraffe$" is not one-to-one. And these two facts are related: as we will see soon, if A is a finite set, and f is a function with domain A, then $\text{Ran}(f)$ has the same number of members as A if and only if f is one-to-one. □

3.2.2 Describing sets and lists by enumeration

Sets and finite lists can be described directly by ***enumerating*** all the members of the set or all the entires of the list, that is, by just writing the names of the members or entries, separated by commas, and

- between ***curly brackets (braces), for sets***, as in the following two examples:
- $\{7, 3, 15, 31\}$ is the set whose members are 3, 7, 15, and 31
- $\{a, c, b\}$ is the set whose members are a, b, c,
- between ***parentheses, for lists***, as in the following two examples:
  - $\{7, 3, 15, 31\}$ is the list of length 4 (i.e., the 4-tuple) whose entries are 7, 3, 15, and 31, in that order.
  - (a, c, b) is the list of length 3 (i.e., the triple) whose entries are a, c, b, in that order.

Notice that, for example,

$$\{7, 3, 15, 31\} = \{3, 7, 31, 15\} = \{3, 7, 3, 15, 31, 3, 7\}\,,$$

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

but

$$(7, 3, 15, 31) \neq (3, 7, 31.15)\,,$$

$$(7, 3, 15, 31) \neq \{3, 7, 3, 15, 31, 3, 7\}\,,$$

and $\quad (a, c, b) \neq (b, a, c)$ and $(a, c, b) \neq (a, c, c, b)\,.$

3.2.3 Describing sets and lists using dummy variable notation

Sets and finite lists can be also be described using ***dummy variable notation***, as in the following examples:

- the set of all prime numbers is the set

$$\{\, n \in \mathbb{N} : n \text{ is a prime number} \,\},$$

or

$$\Big\{\, n \in \mathbb{N} : n > 1 \wedge (\forall m \in \mathbb{N})\Big(m|n \Longrightarrow (m = 1 \vee m = n)\Big) \,\Big\},$$

or

$$\Big\{\, n \in \mathbb{N} : n > 1 \wedge (\forall j \in \mathbb{N})(\forall k \in \mathbb{N})\Big(jk = n \Longrightarrow (j = 1 \vee j = n)\Big) \,\Big\},$$

- the list of the squares of the first ten thousand natural numbers is the list

$$(n_j)_{j=1}^{10{,}000}, \text{ where, for each } j \in \mathbb{N}_{10{,}000}, \; p_j = j^2 .$$

- the list of the first ten thousand prime numbers is the list

$(p_j)_{j=1}^{10{,}000}$, where, for each $j \in \mathbb{N}_{10{,}000}$, p_j is the j-th prime number.

- the list of all the U.S. presidents so far, in chronological order, is the list

$(p_j)_{j=1}^{45}$, where, for each $j \in \mathbb{N}_{45}$, p_j is the j-th U.S. president.

Notice, once again, that

- ***we use curly brackets (i.e., braces), for sets,***
- ***we use parentheses for lists.***

3.3 Finite sets

Definition 42. A finite set is a set A such that

(F) *there exist a nonnegative integer*[a] n *and a function* $f : \mathbb{N}_n \mapsto A$ *such that* $\mathrm{Ran}(f) = A$.

[a] Recall that "nonnegative integer" means "natural number or zero". So "n is a nonnegative integer" means exactly the same as "$n \in \mathbb{N} \cup \{0\}$".

Since, for a function $f : \mathbb{N}_n \mapsto A$, "$f$ is onto A" is equivalent to "$\mathrm{Ran}(f) = A$", Definition 42 is equivalent to the following statement:

A finite set is a set A such that

(F) *there exist a nonnegative integer* n *and a function* $f : \mathbb{N}_n \mapsto A$ *which is onto* A.

And, since "function $f : \mathbb{N}_n \mapsto A$" means "function whose domain is the set $\mathbb{N}_n$ taking values in A", and "function whose domain is $\mathbb{N}_n$" means "finite list of length n", Definition 42 is also equivalent to the following:

A finite set is a set A such that

(F) *there exist a nonnegative integer* n *and a list* L *of length* n *such that* L *is a list of all the members of* A.

3.3.1 What do we mean by "a list of all the members of A"

Definition 43. If $n \in \mathbb{N} \cup \{0\}$, and $L = (a_j)_{j=1}^n$ is a list of length n, we say that

- L is a list of members of A if all the entries of L belong to A, that is, if $a_j \in A$ for every $j \in \mathbb{N}_n$.

- L is a list of all the members of A if all the entries of L belong to A, that is, if $a_j \in A$ for every $j \in \mathbb{N}_n$, and every member of A is an entry of L, that is, if $(\forall a \in A)(\exists j \in \mathbb{N}_n) a = a_j$).

In other words,

- L is a list of members of A if L, regarded as a function, takes values in A (that is, $\mathrm{Ran}(L) \subseteq A$);
- L is a list of all members of A if L, regarded as a function, takes values in A and is onto A (that is, $\mathrm{Ran}(L) = A$).

Example 31. The list $(2, 3, 5, 7, 11)$ is a list of prime numbers, because all the entries of this list are prime numbers.

But $(2, 3, 5, 7, 11)$ is not a list of ***all*** the prime numbers, because, for example, 13 is a prime number but is not an entry of the list. □

3.3.2 Lists without repetitions and one-to-one functions

Definition 44. If $n \in \mathbb{N} \cup \{0\}$ and f is a function such that $\mathrm{Dom}(f) = \mathbb{N}_n$ (that is, f is a list of length n), we say that

- f is a list without repetitions if f is a one-to-one function.

That is, f is a list without repetitions if f there do not exist indices $j \in \mathbb{N}_n$, $k \in \mathbb{N}_n$ such that $j \neq k$ but $f(j) = f(k)$. □

Simply put, f is without repetitions if in f there are no "repeated entries", that is, pairs (j, k) of indices such that $j \neq k$ but $f(j) = f(k)$.

Example 32.

- The list
$$f = (g, i, r, a, f, f, e)$$
has repetitions (that is, is not a list without repetitions), because $f(5) = f(6)$.
- The list
$$g = (g, i, r, a, f, e)$$
is a list wthout repetitions. □

3.3.3 Eliminating repetitions: an example

Example 33. Let A be the set of all U.S. presidents from George Washington to Donald Trump. Since Donald Trump is the 45-th U.S. president, we can define a function $f : \mathbb{N}_{45} \mapsto A$ by letting

$$f(k) = \text{the } \ k-\text{th } \text{ U.S. president, } \text{ for } \ l \in \mathbb{N}_{45}\,.$$

(Using dummy variables list notation, we could equally well have said: "let $f = (p_j)_{j=1}^{45}$, where, for each $j \in \mathbb{N}_{45}$, p_j is the j-th U.S. president".)

So, for example,

$$\begin{aligned} f(1) &= \text{George Washington}\,, \\ f(2) &= \text{John Adams}\,, \\ f(3) &= \text{Thomas Jefferson}\,, \\ &\cdots \\ f(16) &= \text{Abraham Lincoln}\,, \\ &\cdots \\ f(44) &= \text{Barack Obama}\,, \\ f(45) &= \text{Donald Trump}\,. \end{aligned}$$

Then f is a finite list of all the U.S. Presidents. (That is, $f : \mathbb{N}_{45} \mapsto A$ and f is onto A.)

But f is not a one-to-one function (that is, f is not a list without repetitions), because Grover Cleveland is both the 22nd and the 24th U.S. president, so $f(22) = f(24)$. □

How can we create a list g of all the U.S. presidents without repetitions?

The trick is to ***eliminate the repetition (or repetitions, if the list has more than one repetition)***. Here is how you can do that:

Define $g : \mathbb{N}_{44} \mapsto A$ by letting

$$g(k) = \begin{cases} f(k) & \text{if} \quad k \leq 23 \\ f(k+1) & \text{if} \quad k > 23 \end{cases}\,.$$

(In other words: from $k = 1$ up to $k = 23$ we don't change anything, so $g(k)$ is the same as $f(k)$. But for $k = 24$ we start changing things: we do not let $g(24)$ be $f(24)$, because of we did that we would get $g(24) = g(22)$, and there

would be a repetition, What we do instead is ***skip over*** Grover Cleveland, and let $g(24)$ be $f(25)$ (that is we let $g(24)$ =William McKinley, tbe 25-th president of the United States). And the we go on: $g(25)$ is $f(26)$, $g(26)$ is $f(27)$, and so on.)

Then g is a list without repetitions of all the U.S. presidents. (That is, g is a one-to-one function from $\mathbb{N}_{44}$ onto A. So g is a bijection from $\mathbb{N}_n$ to A.) □

3.3.4 Eliminating repetitions: a general theorem

What we did in Example 33 can be done in general. For ***every*** finite list f with repetitions, it is possible to eliminate the repetitions and create a fnite list without repetitions, having the same range as f. We then have the following general theorem.

Theorem 20. *If A is a set, n is a nonnegative integer, and f is a list of length n of all the members of A (that is, $f : \mathbb{N}_n \mapsto A$ and f is onto A), then there exist a nonnegative integer m such that $m \leq n$, and a list g of length m of all the members of A such that g is without repetition (that is, $g : \mathbb{N}_m \mapsto A$, g is onto A, and g is one-to-one).*

Proof. **YOU DO THIS.**

Problem 29. ***Prove*** Theorem 20.

HINT: *In this hint I am basically giving you the whole proof. All you have to do is write it up. But you should write it up well, clearly and precisely.*

What you have to do is eliminate the repetitions that occur in f, one at a time, until there are none left. Read Example 33 above to see how to eliminate one repetition. Then, in your proof, you have to eliminate all the repetitions, one at a time. The best way to do this is with a proof by induction. Prove by induction on n that for every n $P(n)$ is true, where $P(n)$ is the predicate "if A is a set and $f : \mathbb{N}_n \mapsto A$ is a list of length n such that $\text{Ran}(f) = A$, then there exists a list $g : \mathbb{N}_m \mapsto A$ of length m, for some $m \in \mathbb{N} \cup \{0\}$ such that $m \leq n$, such that $\text{Ran}(g) = A$ and g is without repetitions." In the inductive step, when you are assuming $P(n)$ and trying to prove $P(n+1)$, preceed as follows: take $f : \mathbb{N}_{n+1} \mapsto A$ such that $\text{Ran}(f) = A$; if f is without repetitions, take $g = f$ and you are done; if f is with repetitions, eliminate one repetition using the procedure used in

Eaxmple preslist; this results in a list $\tilde{f} : \mathbb{N}_n \mapsto A$ such that $\text{Ran}(\tilde{f}) = A$; and then, by the inductive hypothesis, you can make from $\tilde{f}$ a list $g : \mathbb{N}_n \mapsto A$, for some $m \leq n$, such that $\text{Ran}(g) = A$. □

3.4 Finie sets and bijections

We have defined a "finite set" to be a set A such that

(F) *There exist*

(a) a nonnegative integer n,

(b) a function $f : \mathbb{N}_n \mapsto A$,

such that $\text{Ran}(f) = A$.

And Theorem 20 tells us that, when such n, f exist, wwe can eliminate the repetitions and produce a function $g : \mathbb{N}_m \mapsto A$, for a possibly different n, such that $\text{Ran}(f) = A$, and ***in addition*** g ***is without repetitions, that is,*** g ***is one-to-one.*** This g is also ***onto*** A, becaue $\text{ran}(g) = A$.

So we have proved the following important result.

Theorem 21. *A set A is finite if and only if there exist*

(a) a nonnegative integer n,

(b) a function f,

such that f is a bijection from $\mathbb{N}_n$ to A.

3.5 Infinite sets

Definition 45. A set A is infinite if it is not a finite set.

Problem 30. ***Prove*** that $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are infinite sets. (HINT: Prove by induction on n that is $f : \mathbb{N}_n \mapsto \mathbb{N}$ then $(\exists k \in \mathbb{N})(\forall j \in \mathbb{N}_n) k > f(j)$. Then conclude that f cannot possibly be onto $\mathbb{N}$. A similar strategy works for $\mathbb{Z}$, qq and $\mathbb{R}$ as well.) $\square$

4 Cardinality of sets

4.1 Sets with the same cardinality

If you look at the picture of a bijection on page 77, you can see right away, ***without having to count them***, that the number of squares is exactly the same as the number or circles. This is the crucial insight that leads to the following definition:

Definition 46. Let A, B be sets. We say that

- B has the same number of members as A,

or that

- B has the same cardinality as A,

and write

$$\text{card}(A) = \text{card}(B)\,, \tag{4.106}$$

if there exists a bijection from A to B,

Some authors call two sets "equivalent" if they have the same cardinality in the sense of our defintion. I do not like this because in mathematics there are already too many different meanings of thw word "equivalent" and I do not want to add one more meaning to the list.

Other authors use the word "equipotent", and you are welcome to use it if you wish. I just do not like it so I will not use it.

But it is true that "having the same number of members" is an ***equivalence relation***, in the sense of the following theorem:

Theorem 22. *Let A, B, C be sets. Then:*

(1) A has the same cardinality as A;

(2) if B has the same cardinality as A, then A has the same cardinality as B;

(3) if B has the same cardinality as A, and C has the same cardinality as B, then C has the same cardinality as A,

Proof. To prove (1) we have to show that A has the same cardinality as A, For that purpose, we need a bijection from A to A. But we already know such a bijection, namely, the identity function 1_A. We proved in Theorem 16 that 1_A is a bijection from A to A, so $\boxed{A \text{ has the same cardinality as } A}$.

To prove (2) we have to show that if B has the same cardinality as A, then A has the same cardinality as B. Assume that B has the same cardinality as A, Then there exists a bijection f from A to B. And Theorem 19 tells us that f^{-1} is a bijection from B to A. So there exists a bijection from B to A. Hence $\boxed{A \text{ has the same cardinality as } B}$, and we have proved (2).

Finally, we prove (3). Aasume that B has the same cardinality as A and C has the same cardinality as B. Then there exist a bijection f from A to B and a bijection g from B to C Theorem 14 then tells us that $g \circ f$ is a bijection from A to C. So $\boxed{C \text{ has the same cardinality as } A}$, and (3) is proved. **Q.E.D.**

4.2 Finite sets and their cardinality

Definition 47. If n is a nonnegative integer, and A is a set, we say that A has n members, or that A has cardinality n, or that A is of cardinality n, if there exists a bijection from $\mathbb{N}_n$ to A. □

If we compare this definition with Theorem 21, we see that the following is true:

Theorem 23. *A set A is finite if and only if it is a set of cardinality n for some nonnegative integer n.*

Equivalently, ***a set A is finite if and only if there exist a nonnegative integer n and a bijection from $\mathbb{N}_n$ to A.***

Problem 31. ***Write detailed proofs***, using the definitions, of the following:

1. The empty set is a set of cardinality 0. (HINT: Use Theorem 12.)
2. Any singleton $\{a\}$ is a set of cardinality 1. (HINT: if $A = \{a\}$, define $f : \mathbb{N}_1 \mapsto A$ by letting $f(1) = a$. Prove that f is a bijection from $\mathbb{N}_1$ to A.)
3. An undordered pair $\{a, b\}$ is a set of cardinality 2 if and only if $a \neq b$.
4. An undordered triple $\{a, b, c\}$ is a set of cardinality 3 if and only if $a \neq b$, $a \neq c$, and $b \neq c$.
5. If $n \in \mathbb{N} \cup \{0\}$, then the set $\mathbb{N}_n$ is a set of cardinality n. □

4.2.1 Can we talk about *the* cardinality of a finite set? The fundamental theorem of finite set cardinality theory

Now that we know what a finite set is, we would like to go further and give the following definition: *If A is a finite set and f is a bijection from $\mathbb{N}_n$ to A for some nonnegative integer n, then the number n is said to be the number of members of A, or the cardinality of A.*

But there is a problem. Suppose the following was possible, for some finite set A:

1. m and n are nonnegative integers,
2. there exists a bijection f from $\mathbb{N}_m$ to A,
3. there exists a bijection g from $\mathbb{N}_n$ onto A,
4. $m \neq n$

(For example, there could exist bijections from $\mathbb{N}_{10}$ to A and from $\mathbb{N}_{12}$ to A.)

If this happened, then we would not know which number should be called "***the*** cardinality of A". We would have to talk about "cardinalities of A", accepting that a finite set can have several different cardinalities, in the same way as, for example, an integer can have several factors, and several multiples, so we do not say "6 is *the* factor of 30", or "30 is *the* multiple of 6"; we say "6 is *a* factor of 30" and "30 is *a* multiple of 6".

Fortunately, this problem does not occur. The cardinality of a finite set *is* unique, so we *can* talk about "the" cardinality of a finite set. This is so because of the following theorem:

The fundamental theorem of the theory of finite cardinals

Theorem 24. *Assume that*

1. *A is a set,*
2. *m and n are nonnegative integers,*
3. *there exists a bijection f from $\mathbb{N}_m$ to A,*
4. *there exists a bijection g from $\mathbb{N}_n$ to A.*

Then $m = n$.

Thanks to Theorem 24, if I know that a set A if of cardinality n, then I can say that n is *the* cardinality (or *the* number of members) of A.

Proof of Theorem 24. The key point of the proof is the exchange lemma that we proved earlier as Theorem 13.

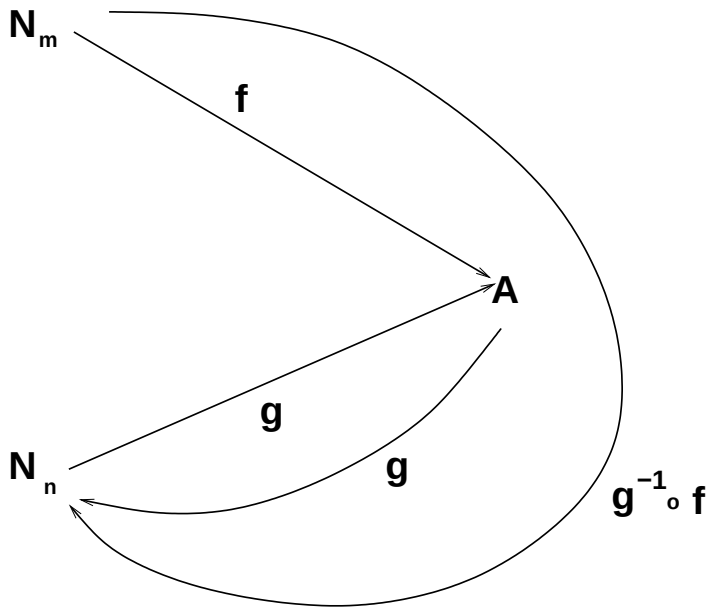
Let us assume that f is a bijection from $\mathbb{N}_m$ to A and g is a bijection from $\mathbb{N}_n$ to A. We want to prove that $m = n$.

Since g is a bijection from $\mathbb{N}_n$ to A, Theorem 19 tells us that g^{-1} is a bijection from A to $\mathbb{N}_n$.

Now we have bijections

$$f : \mathbb{N}_m \mapsto A\,, \quad g^{-1} : A \mapsto \mathbb{N}_n\,.$$

And then Theorem 14 tells us that the composite function $h : \mathbb{N}_m \mapsto \mathbb{N}_n$, defined by $h = g^{-1} \circ f$, is a bijection from $\mathbb{N}_m \mapsto \mathbb{N}_n$.



So all we need to do is prove the following lemma:

Lemma 1. *If $m \in \mathbb{N} \cup \{0\}$, $n \in \mathbb{N} \cup \{0\}$, and there exists a bijection from $\mathbb{N}_m$ to $\mathbb{N}_n$, then $m = n$.*

Proof of Lemma 1. First of all, we look at the case when $m = 0$ or $n = 0$.

Lemma 2. *If*

1. *$m \in \mathbb{N} \cup \{0\}$ and $n \in \mathbb{N} \cup \{0\}$,*
2. *there exists a bijection from $\mathbb{N}_m$ to $\mathbb{N}_n$,*
3. *$m = 0$ or $n = 0$,*

then $m = n$.

Proof. Suppose $m = 0$. Let f be a bijection from $\mathbb{N}_m$ to $\mathbb{N}_n$. Then $\mathrm{Dom}(f) = \mathbb{N}_m$, i.e., $\mathrm{Dom}(f) = \emptyset$. Therefore $f = \emptyset$. So $\mathrm{Ran}(f) = \emptyset$, and then $\mathbb{N}_n = \emptyset$, so $n = 0$. Hence $m = n$, as desired.

Naturally, the same argument works if $n = 0$. So we have proved that $m = n$. **Q.E.D.**

Now assume that m and n are both $\neq 0$. Let h be a bijection from $\mathbb{N}_m$ to $\mathbb{N}_n$. Then by Theorem 13, *there exists a bijection k from $\mathbb{N}_m$ to $\mathbb{N}_n$ that has the additional property that $f(m) = n$.*

But then, if we remove the pair (m, n) from k, we get a bijection from $\mathbb{N}_{m-1}$ to $\mathbb{N}_{n-1}$. So we have proved:

Lemma 3. *If $m \in \mathbb{N}$, $n \in \mathbb{N}$, and there exists a bijection from $\mathbb{N}_m$ to $\mathbb{N}_n$, then there exists a bijection from $\mathbb{N}_{m-1}$ to $\mathbb{N}_{n-1}$.*

Once we have Lemma 3, we can easily prove Lemma 1.

Since there exists a bijection from $\mathbb{N}_m$ to $\mathbb{N}_n$, by Lemma 3 there exists a bijection from $\mathbb{N}_{m-1}$ to $\mathbb{N}_{n-1}$.

If either $m-1 = 0$ or $n-1 = 0$, then Lemma 2 tells us that $m-1 = n-1$, and then $m = n$.

If both $m - 1$ and $n - 1$ are different from zero, so both $m - 1$ and $n - 1$ are natural numbers, then we can apply Lemma 3 again and conclude that there exists a bijection from $\mathbb{N}_{m-2}$ to $\mathbb{N}_{n-2}$.

If either $m-2 = 0$ or $n-2 = 0$, then Lemma 2 tells us that $m-2 = n-2$, and then $m = n$.

If both $m - 2$ and $n - 2$ are different from zero, so both $m - 2$ and $n - 2$ are natural numbers, then we can apply Lemma 3 again and conclude that there exists a bijection from $\mathbb{N}_{m-3}$ to $\mathbb{N}_{n-3}$.

If either $m-3 = 0$ or $n-3 = 0$, then Lemma 2 tells us that $m-3 = n-3$, and then $m = n$.

Continuing in this way, we will eventually find a natural number k such that

(i) $n - k = 0$ or $m - k = 0$.

(ii) there exists a bijection from $\mathbb{N}_{m-k}$ to $\mathbb{N}_{n-k3}$.

Then Lemma 2 tells us that $m - k = n - k$, and then $\boxed{m = n}$.

Thios completes the proof of Theorem 24. **Q.E.D.**

4.2.2 Definition of "cardinality" of a finite set

Now that we have proved Theorem 24, we can talk about *the* cardinality (or *the* number of members) of a finite set A.

Definition 48. Let A be a finite set. Then the nonnegative integer n such that

(*) *there exists a bijection from* $\mathbb{N}_n$ *to* A,

is called the cardinality of A, or the number of members of A. (The number n exists because A is finite, and is unique thanks to Theorem 24.)

We write "card(A)" to denote the cardinality of A. □

Problem 32. ***Prove*** that:

1. If A is a finite set, B is a set, and there exists a bijection from B to A, then B is finite and $\text{card}(B) = \text{card}(A)$.

2. If A and B are finite sets, and $\text{card}(A) = \text{card}(B)$, then there exists a bijection from B to A. □

4.2.3 A trivial but important lemma

The following lemma is very obvious but, as all obvious things is this game, needs proof. The lemma says that if you have a set with n members and remove one member then you are left with a set with $n - 1$ members.

Lemma 4. *If A is a finite set, and a is a member of A, then the set $A - \{a\}$ is finite and has cardinality* $\text{card}(A) - 1$.

Proof. Let $n = \text{card}(A)$. Then we may pick a bijection f from $\mathbb{N}_n$ to A. Thanks to the exchange theorem (i.e., Theorem 13) there exists a bijection g from $\mathbb{N}_n$ to A such that $g(n) = a$.

Let $h = g - \big\{(n, a)\big\}$. (That is, h is the set of ordered pairs obtained from g by removing the pair (n, a).)

Then h is a bijection from $\mathbb{N}_{n-1}$ to $A - \{a\}$. (This is easy to prove. **YOU SHOULD PROVE IT.**)

So $A - \{a\}$ is a finite set and $\text{card}(A - \{a\}) = \text{card}(A) - 1$. **Q.E.D.**

Problem 33. ***Prove*** that the function h that occurs in the proof of Lemma 4 is a bijection from $\mathbb{N}_{n-1}$ to $A - \{a\}$. □

4.2.4 Subsets of a finite set

Definition 49. A proper subset of a set A is a subset B of A such that $B \neq A$. □

Theorem 25. *Let A be a finite set, and let B be a proper subset of A. Then B is finite and* $\text{card}(B) < \text{card}(A)$.

Proof. We will use induction.

Let $P(n)$ be the predicate

$P(n)$ *If A is a finite set with cardinality n, then every proper subset B of A is finite and has cardinality $< n$.*

We prove that $P(n)$ is true for every nonnegative integer n, by induction on n starting at $n = 0$.

Basis step. $P(0)$ is true because, if A if a finite set with cardinality 0, then A must be the empty set, so A has no proper subsets, so the statement "if B is a proper subset of A then B is finite and cars$(B) < 0$" is vacuously true.

Inductive step. Assume $P(n)$ is true.

We want to prove $P(n+1)$. That is, we want to prove that

(#) If A is a finite set with cardinality $n+1$, then every proper subset of A is finite and has cardinality $< n$.

Let A be a finite set with cardinality $n+1$, and let B be a proper subset of A. We want to prove that

(##) B is finite and $\text{card}(B) < n+1$.

Since B is a proper subset of A, $B \neq A$, so there exists $a \in A$ such that $a \notin B$. (Reason: if every member of A was in B, it would follow that $A \subseteq B$. Since $B \subseteq A$, this would imply $B = A$, contradicting our assuption that $B \neq A$.) Let $A' = A - \{a\}$. Then $B \subseteq A'$.

By Lemma 4, A' is a finite set with cardinality n.

The set B is either equal to A' or a proper subset of A'.

If $B = A'$, then B is finite and $\text{card}(B) = n$, so (##) holds.

If B is a proper subset of A' then, by the inductive hypothesis $P(n)$, B is finite and $\text{card}(B) < n$, so *a fortiori* (##) holds.

So (##) holds in both cases. Therefore $P(n+1)$ is true.

This completes the induction, and then the proof of Theorem 25.**Q**.**E**.**D**.

The following is a slightly stronger version of Theorem 25, in which the subset B is not required to be proper.

Theorem 26. *Let A be a finite set, and let B be a subset of A. Then*

1. *B is finite,*
2. *$\text{card}(B) \leq \text{card}(A)$,*
3. *if B is a proper subset of A then $\text{card}(B) < \text{card}(A)$.*

Proof. Let A be a finite set with cardinailty n, and let B be a subset of A. If B is proper, them Theorem 25 tells us that B is finite and $\text{card}(B) < n$.

If B is not proper, then $B = A$, so B is finite and $\text{card}(B) = n$.

So our desired conclusion holds in both cases. **Q.E.D.**

4.2.5 The Dirichlet pigeonhole principle

We are going to use another very important result.

Theorem 27. *Assume that A, B are finite sets and $f : A \mapsto B$ is a one-to-one function. Then*

1. *$\text{card}(A) \leq \text{card}(B)$,*
2. *$\text{card}(A) < \text{card}(B)$ if and only if f is not onto B.*

Theorem 27 is known as the Dirichlet pigeonhole principle (DPHP), for the following reason.

Think of A as a set of pigeons, and B as a set of holes. The function f assigns a hole $f(p)$ to each pigeon p. The fact that f is one-to-one says that different pigeons go to different holes, i.e., that it does no happen that two different pigeons are assigned to the same hole. The theorem then says that

1. there are at least as many holes as there are pigeons,
2. the number of pigeons is equal to the number of holes if and only if every hole is occupied by a pigeon.

Here is another example: suppose that in a classroom there are m students and n seats, and each student is seated, and no seat has more than one student in it. Then the DPHP says that there are at least as many seats as there are students.

Proof of Theorem 27. **YOU DO IT.**

Problem 34. ***Prove*** Theorem 27.

HINT: Let C be the range of f, so C is a subset of B. Prove first that f is a bijection from A to C. Then use Theorems 25 and 26. □

Here is another version of the pigeonhole principle. This time, we look at the case when every hole is occupied by at least one pigeon. The conclusion in this case is that

1. there are at least as many pigeons as there are holes.
2. the number of pigeons is equal to the number of holes if and only if no hole is occupied by more than one pigeon.

Theorem 28. *Assume that A, B are finite sets and $f : A \mapsto B$ is a function onto B. Then*

1. $\text{card}(A) \geq \text{card}(B)$,
2. $\text{card}(A) > \text{card}(B)$ *if and only if f is not one-to-one.*

Proof. **YOU DO IT.**

Problem 35. ***Prove*** Theorem 28.

HINT: Construct a one-to-one "hole-to-pigeon" function by picking for each hole h a pigeon p that occupies hole h. Show that this function is one-to-one and the use Theorem 27. □

Theorem 29. *Let A, B be finite sets. Then*

1. $\text{card}(A) \leq \text{card}(B)$ *if and only if there exists a one-to-one function from A to B,*
2. $\text{card}(A) < \text{card}(B)$ *if and only if there exists a one-to-one function from A to B but there does not exist a one-to-one function from B to B.*

Proof. **YOU DO IT.**

Theorem 30. *Let A, B be finite sets. Then* $\text{card}(A) \leq \text{card}(B)$ *if and only if there exists a function from B onto A.*

1. $\text{card}(A) \leq \text{card}(B)$ *if and only if there exists a function from* B *onto* A,

2. $\text{card}(A) < \text{card}(B)$ *if and only if there exists a function from* B *onto* A *but there does not exist a function from* A *onto* B.

Proof. **YOU DO IT.**

Problem 36. ***Prove*** Theorems 29 and 30. □

4.2.6 Unions of finite sets

Theorem 31. *Let* A, B *be disjoint*[11] *finite sets. Then* $A \cup B$ *is finite, and*

$$\text{card}(A \cup B) = \text{card}(A) + \text{card}(B)\,. \tag{4.107}$$

Proof. **YOU DO IT.**

Problem 37. ***Prove*** Theorem 31.

HINT: You can do this in two ways. One way is to take bijections $f : \mathbb{N}_m \mapsto A$ and $g : \mathbb{N}_n \mapsto B$ and try to cpnstruct from them a bijection $h : \mathbb{N}_{m+n} \mapsto A \cup B$. A second way is to use induction with respect to $\text{card}(A)$ or $\text{card}(B)$. □

Theorem 32. *Let* A, B *be finite sets. Then* $A \cup B$ *is finite, and*

$$\text{card}(A \cup B) = \text{card}(A) + \text{card}(B) - \text{card}(A \cap B)\,. \tag{4.108}$$

Proof. **YOU DO IT.**

Problem 38. ***Prove*** Theorem 32.

HINT: Divide $A \cup B$ intro three sets C, D, E as follows: $C = \{x : x \in A \wedge x \notin B\}$, $D = \{x : x \in B \wedge x \notin A\}$, and $E = A \cap B$. Tnen C, D, F are finite by Theorem 26.

Also, $C \cap E = \emptyset$, $C \cup E = A$, $D \cap E = \emptyset$, $D \cup E = B$, $A \cap D = \emptyset$, $A \cup D = A \cup B$. □

[11] Two sets A, B are disjoint if $A \cap B = \emptyset$.

4.2.7 Sets of subsets

Theorem 33. *Let A be a finite set. Then the power set $\mathcal{P}(A)$ is finite, and*

$$\operatorname{card}\Big(\mathcal{P}(A)\Big) = 2^{\operatorname{card}(A)}\,. \tag{4.109}$$

Proof. **YOU DO IT.**

Problem 39. ***Prove*** Theorem 33.

HINT: Do it by induction on $n = \operatorname{card}(B)$.

Fix $a \in A$, and let $A' = A - \{a\}$. Then the subsets of A are of two kinds: those that do not contain a as a member and those that do. The subsets of the first kind are exactly the subsets of A', so by the inductive hyptohesis there are 2^{n-1} such sets. If $\mathcal{B}$ is the set of all the subsets of the second kind, then you should construct a bijection from $\mathcal{B}$ to $\mathcal{P}(A')$. Then $\mathcal{P}(A) = \mathcal{P}(A') \cup \mathcal{B}$, $\mathcal{P}(A') \cap \mathcal{B} = \emptyset$, and $\operatorname{card}(\mathcal{B}) = \operatorname{card}\big(\mathcal{P}(A')\big)$. □

4.2.8 Cartesian products of finite sets

Theorem 34. *Let A, B be finite sets. Then $A \times B$ is finite, and*

$$\operatorname{card}(A \times B) = \operatorname{card}(A) \cdot \operatorname{card}(B)\,. \tag{4.110}$$

Proof. **YOU DO IT.**

Problem 40. ***Prove*** Theorem 34.

HINT: Do it by induction on $m = \operatorname{card}(B)$.

Prove that if $b \in B$, and $B' = B - \{b\}$, then

$$A \times B = (A \times B') \cup (A \times \{b\})\,, \text{ and } (A \times B') \cap (A \times \{b\}) = \emptyset\,.$$

and use this in your inductive argument. □

4.3 Infinite sets

We recall the definition of "infinite set": *A set is infinite if it is not a finite set.*

Theorem 35. *The set* $\mathbb{N}$ *of all natural numbers is infinite.*

In Problem 30, on page 96, I gave you hints for one proof of Theorem 35. Here I am giving you another proof, based on the Dirichlet pigeonhole principle.

Idea of the proof. If $\mathbb{N}$ was finite, then it would have some cardinality $n \in \mathbb{N} \cup \{0\}$, and this means that we can pick a pigeon p_k for each $k \in \mathbb{N}$ and fit all these pigeons in n holes. But $\mathbb{N}$ has at least m members, for every m. So for every m we can fit m pigeons in n holes. So $m \geq n$ by the Dirichlet pigeonhole principle. So the number n is greater than every natural number, But such an n cannot exist.

Now let us write this down in mathematical language.

Proof.

Suppose $\mathbb{N}$ was finite.
Then there exist a natural number n and a bijection f from $\mathbb{N}_n$ to $\mathbb{N}$.
The inverse function $g = f^{-1}$ is then a bijection from $\mathbb{N}$ to $\mathbb{N}_n$.
Now let m be an arbitrary natural number.
Define a function g_m, with domain $\mathbb{N}_m$, by letting

$$g_m(k) = g(x) \text{ for } k \in \mathbb{N}_m\,.$$

Then $g_m : \mathbb{N}_m \mapsto \mathbb{N}$ and g_m is one-to-one. (Proof: if $k_1, k_2 \in \mathbb{N}_m$ and $g_m(k_1) = g_m(k_2)$ then $g(k_1) = g(k_2)$, so $k_1 = k_2$ because g is one-to-one.

Furthermore, $g : \mathbb{N}_m \mapsto \mathbb{N}_n$. It the follows from the Dirichlet pigeonhole principle (Theorem 27) that $n \geq m$.
Since m was an arbitrary natural number, we have proved that

$$(\forall m \in \mathbb{N}) n \geq m\,. \tag{4.111}$$

So we have found a natural number n which is larger than every natural number.
But we know that such a number cannot exist. (That is, (4.111) is impossible. This is easily seen as follows: if (4.111) was true for some $n \in \mathbb{N}$, then we could specialize to $m = n + 1$ and conclude that $n \geq n + 1$. But $n < n + 1$, so we have arrived at a contradiciton.)

So the assumption that $\mathbb{N}$ is finite has led us to a contradiction.**Q**.**E**.**D**.

Theorem 36. *If A, B are sets, f is a bijection from A to B, and A is infinite, then B is infinite.*

Proof. **YOU DO THIS.**

Problem 41. ***Prove*** theorem 36. □

Theorem 37. *If A is a set, B is a subset of A, and B is infinite, then A is infinite.* □

Proof. **YOU DO THIS.**

Problem 42. ***Prove*** theorem 37. □

Theorem 38. *Define a function f from $\mathbb{N}$ to $\mathbb{Z}$ as follows:*

$$f(n) = \begin{cases} \frac{n}{2} & \text{if} \quad n \in \mathbb{N} \text{ and } n \text{ is even} \\ \frac{1-n}{2} & \text{if} \quad n \in \mathbb{N} \text{ and } n \text{ is odd} \end{cases} . \tag{4.112}$$

Then f is a bijection from $\mathbb{N}$ to $\mathbb{Z}$.

Proof. **YOU DO THIS.**

Problem 43. ***Prove*** Theorem 38. □

Problem 44. Let $\mathcal{E}_{>0}$ be the set of all even natural numbers. That is,

$$\mathcal{E}_{>0} = \{n \in \mathbb{N} : 2|n\}, \tag{4.113}$$

and let $\mathcal{E}$ be the set of all even integers, so

$$\mathcal{E} = \{n \in \mathbb{Z} : 2|n\}, \tag{4.114}$$

Construct bijections from $\mathbb{N}$ to $\mathcal{E}_{>0}$ and from $\mathbb{N}$ to $\mathcal{E}$. □

NOTE: If f is a function whose domain in $\mathbb{N} \times \mathbb{N}$, the set of all order pairs (m, n) of natural numbers, and u is a member of the domain of f, we have to write $f(u)$ for the value of f at u. But u is itself an ordered pair (m, n), so we should write $f\big((m, n)\big)$ for the value of f at u. i.e., at (m, n). But we are going to follow the starnard practice of omitting one pair of parentheses and just write "$f(m, n)$", instead of "$f\big((m, n)\big)$".

Theorem 39. *Define a function f from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$ as follows:*

$$f(m, n) = 2^{m-1}(2n - 1) \text{ for} \tag{4.115}$$

Then f is a bijection from from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$.

Proof. **YOU DO THIS.**

Problem 45. ***Prove*** Theorem 39. □

Problem 46. ***Construct*** a partition of $\mathbb{N}$ into infinitely many infinite sets.

NOTE: A partition of a set A is a set $\mathbf{P}$ such that

1. $\mathbf{P} \neq \emptyset$,
2. $\emptyset \notin \mathbf{P}$ (that is, every member of $\mathbf{P}$ is nonempty),
3. every member of A is in S for some $S \in \mathbf{P}$,
4. if S, T are any two different members of $\mathbf{P}$, then $S \cap T = \emptyset$.

An example of a partition of $\mathbb{N}$ is given by letting $\mathbf{P} = \{E, O\}$, where E is the set of all even natural numbers and O is the set of all odd natural numbers.

Another example of a a partition of $\mathbb{N}$ is given by letting $\mathbf{P}$ be the set whose members are all the singletons $\{n\}$, for all $n \in \mathbb{N}$. (That is, $\mathbf{P} = \{\, X : (\exists n \in \mathbb{N}) X = \{n\} \,\}$.)

In the first example, the partition $\mathbf{P}$ is a finite set, and the members of $\mathbf{P}$ are infinite sets. In the second example, the partition $\mathbf{P}$ is an infinite set, but the members of $\mathbf{P}$ are finite sets.

What I am asking you to do is construct a partition $\mathbf{P}$ which is an infinite set and is such that all the members of $\mathbf{P}$ are infinite sets.

HINT: Using the result of Theorem 39, this should juat require two or three lines. □

Theorem 40. *There exists a bijection from* $\mathbb{N}$*, the set of all naatural numbers, to* $\mathbb{Q}$*, the set of all rational numbers.*

Proof. This proof is done in the book. You should look it up there.

Problem 47. ***Prove*** that there exists a bijection from $\mathbb{N}$ to $\mathbb{Q} \times \mathbb{Q}$. □

4.3.1 Countable sets

Definition 50.

- A set A is countable if there exists a one-to-one function $f : A \mapsto \mathbb{N}$.
- A set A is countably infinite if it is countable and infinite. □

Example 34. It is clear that

1. $\mathbb{N}$ *is countable.* (Proof: the function $1_{\mathbf{N}}$ is a bijection from $\mathbb{N}$ to $\mathbb{N}$, so in particular it is a one-to-one function from $\mathbb{N}$ to $\mathbb{N}$.
2. *Every subset of a countable set is countable.* (Proof: Let A be countable, and let B be a subset of A. Let $f : A \mapsto \mathbb{N}$ be a one-to-one function. Define $g : B \mapsto \mathbb{N}$ by letting $g(x) = f(x)$ for each $x \in B$. Then g is one-to-one.)
3. *Every finite set is countable.*
4. $\mathbb{N}$ *is countably infinite.* (Proof: $\mathbb{N}$ is countable, and $\mathbb{N}$ is infinite because of Theorem 35.)
5. If A, B are sets and f is a bijection from A to B, then A is countably infinite if and only if B is.
6. $\mathbb{Z}$*,* $\mathbb{N} \times \mathbb{N}$*, and* $\mathbb{Q}$ *are countably infinite.* (Reason: we have already constructed bijections from $\mathbb{N}$ to $\mathbb{Z}$ and from $\mathbb{N}$ to $\mathbb{N} \times \mathbb{N}$, and Theorem 40 tells us that there exists a bijection from $\mathbb{N}$ to $\mathbb{Q}$.)
7. The set of all prime numbers is countably infinite. (Indeed, we have proved earlier in the course that the set if infinite. And in addition it is a subset of $\mathbb{N}$, so it is countable.) □

4.3.2 Do all infinite sets have the same cardinality?

The results of Theorems 38, 39 and problems 44 show that sets as diverse as $\mathbb{Z}$, $\mathcal{E}_{>0}$, $\mathcal{E}$, and $\mathbb{N} \times \mathbb{N}$, some of which (for example, $\mathbb{Z}$ and $\mathbb{N} \times \mathbb{N}$) appear to be much larger than $\mathbb{N}$, have in fact the same cardinality as $\mathbb{N}$.

Could it be that all infinite sets have the same cadinality as $\mathbb{N}$?

The asnwer is a resounding NO!!!. Here is a result which is very easy to prove but has momentous consequences.

Theorem 41 *(Cantor) If X is a set, then there does not exist a function from X onto the power set $\mathcal{P}(X)$.*

Proof of Cantor's Theorem.

Suppose $f : X \mapsto \mathcal{P}(X)$ is onto $\mathcal{P}(X)$.

Let

$$S = \{x \in X : x \notin f(x)\}.$$

Then S is a subset of X, so $S \in \mathcal{P}(X)$.

Since f is onto $\mathcal{P}(X)$, we can pick $s \in X$ such that $f(s) = S$.

We are going to prove that $s \in S \wedge s \notin S$.

First, lve that $s \in S$.

Suppose $s \notin S$.

Then $s \notin f(s)$, so s satisfies the membership criterion for S ("$x \notin f(x)$").

Therefore $s \in S$.

> But we are assuming that $s \notin S$, so we have reached a contradiction.

So the assumption that $s \notin S$ had led us to a contradiction, and then it follows that $\boxed{s \in S}$.

Now let us prove that $s \notin S$:

> Suppose $s \in S$.
>
> Then $s \in f(s)$, so s does not satisfy the membership criterion for S ("$x \notin f(x)$").
>
> Therefore $s \notin S$.
>
> But we are assuming that $s \in S$, so we have reached a contradiction.

So the assumption that $s \in S$ had led us to a contradiction, and then it follows that $\boxed{s \notin S}$.

We have proved that $\boxed{s \in S \wedge s \notin S}$. So we have arrived at a contradiction. The contradiction resulted from assuming that there exists a function f from X onto $\mathcal{P}(X)$. Hence $\boxed{\text{a function } f \text{ from } X \text{ onto } \mathcal{P}(X) \text{ does not exist}}$. **Q.E.D.**

4.3.3 Consequences of Cantor's Theorem

Theorem 41 says that if X is any set then there does not exist a function from X onto $\mathcal{P}(X)$. So in particular there cannot exist a bijection from X to $\mathcal{P}(X)$.

This means that the sets X and $\mathcal{P}(X)$ do not have the same cardinality. Can we say that one of them is "larger" than the other one? The answer is "yes", $\mathcal{P}(X)$ definitely has a larger cardinality than X. But before we say that, we have to know what it means: ***what does it mean for a set A to have a larger cardinality than that of a set B?***

In order to asnwer that question, we first look at what happens for finite sets:

(I) First of all, if A and B are finite sets, then the cardinalities $\text{card}(A)$ and $\text{card}(B)$ are nonnegative integers, and we know what it means for a nonnegative integer to be larger than another nonnegative integer.

(II) Second, Theorem 29 tells us that, if A and B are finite sets, then

1. $\text{card}(A) \leq \text{card}(B)$ if and only if there exists a one-to-one function from A to B,
2. $\text{card}(A) < \text{card}(B)$ if and only if there exists a one-to-one function from A to B but there does not exist a one-to-one function from B to B.

The conditions of (II) make perfect sense for infinite sets as well, even though we do not know what "$\text{card}(A)$" means. (We have only defined what it means for two sets A, B to "have the same cardinality". This does not say that there is some object called "the cardinality of a set", and that two sets have the same cardinality if and only if that object is the same for both. For finite sets, we were able to define such an object, and it turned out to be a nonnegative integer. For infinite sets, this can be done too, but we have not done it yet, so at this point we do not know what "$\text{card}(A)$" means. All we know is what "$\text{card}(A) = \text{card}(B)$" means. And in the next section we are going to assign a menaning to "$\text{card}(A) \leq \text{card}(B)$", "$\text{card}(A) < \text{card}(B)$", "$\text{card}(A) \geq \text{card}(B)$", and "$\text{card}(A) > \text{card}(B)$", but we will still not know what "$\text{card}(A)$" means.

4.3.4 Comparing sizes of sets. The Cantor-Schroeder-Bernstein Theorem

We follow the idea of Theorem 29. (We could also follow the second one, and it works, but there are some complications.)

Definition 51. Suppose that Let A, B are sets.

- We say that A has cardinality smaller than or equal to that of B, or that B has cardinality larger than or equal to that of A, and write

$$\text{card}(A) \leq \text{card}(B)\,,$$

or

$$\text{card}(B) \geq \text{card}(A)\,,$$

if there exists a one-to-one function from A to B.

- We say that A has cardinality strictly smaller than that of B, or that B has cardinality strictly larger than that of A, or that and write

$$\mathrm{card}(A) < \mathrm{card}(B)$$

or

$$\mathrm{card}(B) > \mathrm{card}(A)\,,$$

if there exists a one-to-one function from A to B, but there does not exist a bijection from A to B. □

As an important example of the use of these definitions, we prove the following theorem.

Theorem 42 *(Cantor) If X is a set, then the cardinality of X is strictly smaller than the cardinality of the power set $\mathcal{P}(X)$. That is:*

$$\mathrm{card}(X) < \mathrm{card}\big(\mathcal{P}(X)\big)\,. \tag{4.116}$$

Proof. First, we show that $\mathrm{card}(X) \le \mathrm{card}\big(\mathcal{P}(X)\big)$, by constructing a one-to-one function $f : X \mapsto \mathcal{P}(X)$.

This is very easy: define $f : X \mapsto \mathcal{P}(X)$ by letting

$$f(x) = \{x\} \qquad \text{for} \quad x \in X\,.$$

Then f is clearly one-to-one. (Proof: suppose $x_1, x_2 \in X$ and $f(x_1) = f(x_2)$; then $\{x_1\} = \{x_2\}$; since $x_2 \in \{x_2\}$, it follows that $x_2 \in \{x_1\}$; but x_1 is the only member of $\{x_1\}$; so $x_2 = x_1$.)

So we have constructed a one-to-one function from X to $\mathcal{P}(X)$.

On the other hand, Theorem 41 tells us that there does not exist a function from X onto $\mathcal{P}(X)$. In particular, there does not exist a bijection from X to $\mathcal{P}(X)$.

This proves that (4.116) holds. **Q.E.D.**

The relations "$\leq$", "$\geq$", "$<$", "$>$", should behave like their homonyms[12] the relations "$\leq$", "$\geq$", "$<$", "$>$", between real numbers.

So, for example, we would expect that there is a true theorem about inequalities among cardinals corresponding to each of the following properties of inequalities between real numbers:

(R1) If $a, b \in \mathbb{R}$, then $a \leq b$ if and only if $b \geq a$.
(R2) If $a, b \in \mathbb{R}$, then $a < b$ if and only if $b > a$.
(R3) If $a, b, c \in \mathbb{R}$, $a \leq b$, and $b \leq c$, then $a \leq c$.
(R4) If $a, b \in \mathbb{R}$, then $a \leq b$ if and only if $a < b$ or $a = b$.
(R5) If $a, b \in \mathbb{R}$ and $a < b$, then $a \neq b$.
(R6) If $a, b \in \mathbb{R}$, $a \leq b$, and $b \leq a$, then $a = b$.
(R7) If $a, b, c \in \mathbb{R}$, $a \leq b$, $b \leq c$, and either $a < b$ or $b < c$, then $a < c$.
(R8) If $a, b \in \mathbb{R}$, then either $a \leq b$ or $b \leq a$.

It turns out that ***the analogues of the nine properties listed above are all true; some are trivially true, but others are not at all obvious and their proofs require a lot of work.***

Let us start with the obvious ones: the analogues of (R1), (R2), (R3), (R4), (R5) for cardinalities are trivially true. We say that in the following theorem:

Theorem 43. *Let A, B, C be sets. Then*

(C1) $\operatorname{card}(A) \leq \operatorname{card}(B)$ *if and only if* $\operatorname{card}(A) \geq \operatorname{card}(B)$.

(C2) $\operatorname{card}(A) < \operatorname{card}(B)$ *if and only if* $\operatorname{card}(B) > \operatorname{card}(A)$.

(C3) If $\operatorname{card}(A) \leq \operatorname{card}(B)$ *and* $\operatorname{card}(B) \leq \operatorname{card}(C)$ *then* $\operatorname{card}(A) \leq \operatorname{card}(C)$

[12] ***Homonyms*** are words or symbols that are spelled or written identically but have different meanings. For example, "crane", a mechanical lifting machine, and "crane", a bird, are homonyms. Mathematics is full of homonyms. For example, "$<$" as a binary relation between real numbers, and "$<$" as a binary relation between cardinalities, are different meanings of the symbol "$<$".

(C4) $\operatorname{card}(A) \leq \operatorname{card}(B)$ *if and only if either* $\operatorname{card}(A) < \operatorname{card}(B)$ *or* $\operatorname{card}(A) = \operatorname{card}(B)$.

(C5) If $\operatorname{card}(A) < \operatorname{card}(B)$ *then it's not true that* $\operatorname{card}(A) = \operatorname{card}(B)$.

Proof. Statement (C1) is true because Definition 51 tells us "$\operatorname{card}(A) \leq \operatorname{card}(B)$" and "$\operatorname{card}(B) \geq \operatorname{card}(A)$" are two ways of writing the same thing.

Similarly, statement (C2) is true because Definition 51 tells us "$\operatorname{card}(A) < \operatorname{card}(B)$" and "$\operatorname{card}(B) > \operatorname{card}(A)$" are two ways of writing the same thing.

To prove (C3), assume that $\operatorname{card}(A) \leq \operatorname{card}(B)$ and $\operatorname{card}(B) \leq \operatorname{card}(C)$. This means, according to Definition 51, that there exist one-to-one functions $f : A \mapsto B$ and $g : B \mapsto C$. Then the composite $g \circ f$ is a function from A to C, and Theorem 10 tells us that $g \circ f$ is one-to-one. Hence $g \circ f$ is a one-to-one function from A to C. So $\operatorname{card}(A) \leq \operatorname{card}(C)$.

Next, we prove (C4). Wew have to prove that

$$\operatorname{card}(A) \leq \operatorname{card}(B) \Longleftrightarrow \big(\operatorname{card}(A) < \operatorname{card}(B) \vee \operatorname{card}(A) = \operatorname{card}(B)\big)\,. \tag{4.117}$$

To prove (4.117) we prove the implications

$$\operatorname{card}(A) \leq \operatorname{card}(B) \Longrightarrow \big(\operatorname{card}(A) < \operatorname{card}(B) \vee \operatorname{card}(A) = \operatorname{card}(B)\big)\,. \tag{4.118}$$

and

$$\big(\operatorname{card}(A) < \operatorname{card}(B) \vee \operatorname{card}(A) = \operatorname{card}(B)\big) \Longrightarrow \operatorname{card}(A) \leq \operatorname{card}(B)\,. \tag{4.119}$$

Finally, we have to prove (C5). But (C5) is completely trivial: by definition, "$\operatorname{card}(A) < \operatorname{card}(B)$" means "there is a one-to-one function from A to B but there is no bijection from A to B". So in particular if $\operatorname{card}(A) < \operatorname{card}(B)$ then there is no bijection from A to B, so it's not true that $\operatorname{card}(A) \leq \operatorname{card}(B)$. **Q.E.D.**

To prove the analogues of (R6), (R7), and (R8), we need deeper results from set theory.

Let us start with (C6), the analogue for cardinalities of property (R6). We need to prove that

(&) *if* $\operatorname{card}(A) \leq \operatorname{card}(B)$ *and* $\operatorname{card}(B) \leq \operatorname{card}(A)$ *then* $\operatorname{card}(A) = \operatorname{card}(B)$.

Translating this into English, (&) says:

(&&) *if there exist one-to-one functions* $f : A \mapsto B$, $g : B \mapsto A$, *then there exists a bijection from* A *to* B.

And we have to asnwer the question: ***is (&&true?***.

For finite sets the answer is undoubtedly "'yes": if A, B have cardinalities m, n, and there exist one-to-one functions $f : A \mapsto B$, $g : B \mapsto A$, then it follows from the Dirichlet pigeonhole principle that $m \leq n$ and $n \leq m$, , so $m = n$, and this implies that there exists a bijection from A to B.

Actually, even more can be proved:

Theorem 44. *If* A, B *are finite sets, and* $f : A \mapsto B$, $g : B \mapsto A$ *are one-to-one functions, then* f *is a bijection from* A *to* B *and* g *is a bijection from* B *to* A.

Proof. The range $\mathrm{Ran}(f)$ of f is a subset of A, and f is a bijection from A to $\mathrm{Ran}(f)$.

Assume that $\mathrm{Ran}(f)$ is a proper subset of B, then $\mathrm{card}(\mathrm{Ran}(f)) < \mathrm{card}(B)$ by Theorem 25, while on the other hand $\mathrm{card}(\mathrm{Ran}(f)) = \mathrm{card}(A)$, so $\mathrm{card}(A) < \mathrm{card}(B)$, and then the Dirichlet pigeonhole principle tells us that there cannot exist a one-to-one function from B to A. Since g is a one-to-one function from B to A, the assumptiom that $\mathrm{Ran}(f)$ is a proper subset of B has led us to a contradiction.

So $\mathrm{Ran}(f) = B$, and then f is onto B. A similar argument proves that g is onto A. **Q.E.D.**

For infinite sets, the analogue of Theorem 44 is not true. Here is a sumple example. Let $\mathcal{E}$ be the set of all even natural numbers. Define $f : \mathbb{N} \mapsto \mathcal{E}$, and $g : \mathcal{E} \mapsto \mathbb{N}$ by letting

$$\begin{aligned} f(n) &= 4n \qquad \text{for} \quad n \in \mathbb{N}\,, \\ g(n) &= n \qquad \text{for} \quad n \in \mathcal{E}\,. \end{aligned}$$

Then $f : \mathbb{N} \mapsto \mathcal{E}$, and $g : \mathcal{E} \mapsto \mathbb{N}$ aare one-to-one functions but neither one is a bijection.

And yet, even though f and g are not themselves bijecyion, a bijection from $\mathbb{N}$ to $\mathcal{E}$ does exist: just define $h : \mathbb{N} \mapsto \mathcal{E}$ by letting $h(n) = 2n$, and it is clear that h is a bijection from $\mathbb{N}$ to $\mathcal{E}$.

It turns out that what happened in this example actually does happen in general.

Theorem 45 *(Cantor-Schroeder-Bernstein) If A, B are sets and and $f : A \mapsto B$, $g : B \mapsto A$ are one-to-one functions, then there exists a bijection from A to B.*

The proof of this theorem is given in the book, and I am not going to do it here.

Thanks to the Cantor-Schroeder-Bernstein theorem, statement (&&) above is true, and this implies that condition (C6), the analogue for sets of property (R6), is true. So we get the following theorem:

Theorem 46. *Let A, B be sets such that* $\text{card}(A) < \text{card}(B)$. *Then* $\sim \text{card}(A) = \text{card}(B)$*, that is, B does not have the same cardinality as A.*

(*We do not give a proof, because we have already proved this.*

We now turn to (C7), the cardinality analogue of (R7).

Theorem 47. *If A, B, C are sets such that* $\text{card}(A) \leq \text{card}(B)$, $\text{card}(B) \leq \text{card}(C)$*, and one of the inequalities is strict (that is, either* $\text{card}(A) < \text{card}(B)$ *or* $\text{card}(B) < \text{card}(C)$*) then* $\text{card}(A) < \text{card}(C)$.

Proof. Assume that $\text{card}(A) \leq \text{card}(B)$ and $\text{card}(B) \leq \text{card}(C)$. Then we pick one-to-one functions $f : A \mapsto B$ and $g : B \mapsto C$.

We want to prove that if one of the inequalities is strict, then $\text{card}(A) < \text{card}(C)$.

We already know from Theorem 43, condition (C3), that $\text{card}(A) \leq \text{card}(C)$, and this means that either $\text{card}(A) < \text{card}(C)$ or $\text{card}(A) = \text{card}(C)$.

So, in order to prove that $\text{card}(A) < \text{card}(C)$, we have to exclude the possibility that $\text{card}(A) = \text{card}(C)$.

Suppose that $\text{card}(A) = \text{card}(C)$. Then there exist bijections h, k, from A to C and from C to A, respectively.

So we have functions

$$f : A \mapsto B\,,\ \ g : B \mapsto C\,,\ \ h : A \mapsto C\,,\ \ k : C \mapsto A\,,$$

such that f and g are one-to-one and h and k are bijections.

Since the composite of two one-to-one functions is one-to-one, the composite function $k \circ g : B \mapsto A$ is one-to-one. So we have one-to-one functions $f : A \mapsto B$, $k \circ g : B \mapsto A$. Then the Cantor-Schroeder-Bernstein theorem tells us that there exists a bijection from A to B so $\boxed{\text{card}(A) = \text{card}(B)}$.

Similarly, the composite function $f \circ k : C \mapsto B$ is one-to-one. So we have one-to-one functions $g : B \mapsto C$, $f \circ k : C \mapsto B$. Then the Cantor-Schroeder-Bernstein theorem tells us that there exists a bijection from B to C so $\boxed{\text{card}(B) = \text{card}(C)}$.

So we have proved that both $\text{card}(A) = \text{card}(B)$ and $\text{card}(B) = \text{card}(C)$. And this contradicts the assumption either $\text{card}(A) < \text{card}(B)$ or $\text{card}(B) < \text{card}(C)$.

This contradction arose from assuming that $\text{card}(A) = \text{card}(C)$. Hence it is not true that $\text{card}(A) = \text{card}(C)$. **Q.E.D.**

Finally, we need the cardinality analogue of (R8). This is indeed true, and we state it as a theorem:

Theorem 48. *If A, B are sets, then* $\text{card}(A) \leq \text{card}(B)$ *or* $\text{card}(B) \leq \text{card}(A)$. *That is, one of the following is true:*

- *there exists a one-to-one function from A to B,*
- *there exists a one-to-one function from B to A.*

The proof of this theorem requires methods that are above the level of this course. So here we just leave the theorem without proof.

4.3.5 Infinitely many infinite cardinals

It follows from Theorem 42 that

Theorem 49 *The power set $\mathcal{P}(\mathbb{N})$ is not countable.*

So there are are least two different infinite cardinals: that of $\mathbb{N}$ (and all countably infinits sets), and that of $\mathcal{P}(\mathbb{N})$. But then it is clear that there are many more, in fact infinitely many more, because we can consider the sets

$$\mathbb{N}\,,\ \mathcal{P}(\mathbb{N})\,,\ \mathcal{P}\Big(\mathcal{P}(\mathbb{N})\Big)\,,\ \mathcal{P}\Big(\mathcal{P}\Big(\mathcal{P}(\mathbb{N})\Big)\Big)\,,\ \mathcal{P}\left(\mathcal{P}\Big(\mathcal{P}\Big(\mathcal{P}(\mathbb{N})\Big)\Big)\right),\cdots.$$

That is, we can define, inductively,

$$\begin{aligned}\mathcal{P}_0(\mathbb{N}) &= \mathbb{N}\,,\\ \mathcal{P}_{n+1}(\mathbb{N}) &= \mathcal{P}\Big(\mathcal{P}_n(\mathbb{N})\Big) \ \text{ for } \ n\in\mathbb{Z}\,,\, n\geq 0\,,\end{aligned}$$

and in this way we obtain an infinite sequence $\Big(\mathcal{P}_n(\mathbb{N})\Big)_{n=1}^{\infty}$ of sets each one of which has cardinality strictly larger than the previous obe.

But the story does not end there. We can construct an enormous set $\mathcal{P}_\infty(\mathbb{N})$, defined by

$$\mathcal{P}_\infty(\mathbb{N}) = \bigcup_{n=0}^{\infty}\mathcal{P}_n(\mathbb{N})\,,$$

and then stasrt again, contructiong the sets $\mathcal{P}_n\left(\big(\mathcal{P}_\infty(\mathbb{N})\big)\right)$, and so on.

The result is an infinite tower of infinite towers of infinite towers ,,,, of infinite cardinals.

5 The paradoxes of set theory: Russell's paradox and others

In the story I have been telling you so far there are serious problems.

5.0.6 The Cantor paradox

We said that the cardinality of the power set of a set X is strictly larger than the cardinality of X. But ***what if we apply this to the set of all sets?***

That is, let

$$X = \Big\{ x : x \text{ is a set} \Big\}.$$

Then we have seen that $\boxed{\text{card}\big(\mathcal{P}(X)\big) > \text{card}(X)}$.

But $\mathcal{P}(X)$ is a set whose members are sets, so $\mathcal{P}(X)$ is a subset of X, and then $\boxed{\text{card}\big(\mathcal{P}(X)\big) \leq \text{card}(X)}$.

So we get a contradiction! And this time we have done nothing wrong!

5.0.7 The Russell paradox

Here is another way to get a contradiction in Set Theory. It is the famous ***Russell paradox.***

Let X be the set of all sets that are not members of themselves. That is, we let

$$X = \{x : x \text{ is a set } \wedge\, x \notin x\}\,.$$

Let us prove that $X \in X$. Suppose that $\boxed{X \notin X}$. Then is a set that is not a member of itself. So X satisfies the membership criterion for X. Hence $X \in X$. But we are assuming that $X \notin X$. So $\boxed{X \in X \wedge X \notin X}$, which is a contradiction.

So the assumption that $X \notin X$ has led us to a contradiction. Hence $\boxed{\boxed{X \in X}}$.

Now let us prove that $X \notin X$. Suppose that $\boxed{X \in X}$. Then is a set that is a member of itself. So X does not satisfy the membership criterion for X. Hence $X \notin X$. But we are assuming that $X \in X$. So $\boxed{X \in X \wedge X \notin X}$, which is a contradiction.

So the assumption that $X \in X$ has led us to a contradiction. Hence $\boxed{X \notin X}$.

So we have proved that $X \in X \wedge X \notin X$, which is a contradiction.

So

> In set theory it is possible to prove a contradiction.

And, once you have proved a contradiction, then everything csn be proved, because:

> In a theory in which it is possible to prove a contradiction, it is possible to prove every statement, whether it is true or false.

This is so for a simple reason: take any statement S you want (for example, S could be "$2+2=5$", or "6 is a prime number", or "the 45th president of the U.S. is Hillary Clinton", or "the Earth hs flat and rests on top of a giant turtle".

Let us prove S, assuming we know how to prove a contradction C.

To prove S, you do it by contradiction: start with "Assume $\sim S$". Then insert your proof of C, ending with C. So, you see, assuming $\sim C$ we got a contradiction. Therefore we have proved S. **Q.E.D.**

What is wrong with this. Isn't is wonderful that we can prove everything? Shouldn't we celebrate? No more having to study hard to learn how to prove things!!! We have an easy method for proving everything, without doing any work!

The trouble is,

A theory in which it is possible to prove everything is completely worthless.

The purpose of writing proofs is to make sure that the mathematical statements we write are true. If we prove something, then we can be sure it is true, because the rules of logic are designed to guarantee that everything we prove is true.

The catch is: if we can prove everything, including statements that are false, then the fact that we have proved something tells us nothing: it could be true or it could be false.

Think of theorem-proving as analogous to smoke-detecting.

A naïve person might think that, since the purpose of a smoke detector is to detect smoke, a device that rings every time there is smoke is precisely what is desired of a good smoke detector.

However, it may happen that the device rigns every time there is smoke because it rings all the time,whetehr there is smoke or not.

Such a "smoke detector" is useless. What you want is a device that rings when there is smoke and does not rignt when there is no smoke. That way, when you hear the device ring, you know that there is smoke.

Similarly, theorem-proving is useful if you can prove the statements that are true, and you cannot prove those that are not true. If you can prove too muc=h, if you can prove assertion that are false, then your theorem-proving has absolutely no value.

5.0.8 The need for Axiomatic Set Theory

The trouble with the paradoxes of the last section arose from the fact that we made indiscriminate use of the Axiom of Set Formation. The axiom says that "if we take any one-variable predicate $P(x)$, we can form the set $\{x : P(x)\}$." Using this, we created the sets $\{x : x \text{ is a set}\}$ (the set of all sets) and $\{x : x \text{ is a set} \wedge x \notin x\}$ (the set of all sets that do not belong to themselves). And these sets led us to contradictions.

The solution that mathematicians have adopted is to develop "Axiomatic Set Theory" (AST). In AST, axioms are stated that tell us under what

conditions is is possible to create a set. And the axioms are carefully chosen so that the sets that caused us trouble cannot be formed.

But this should be the subject of another course.

6 Some more problems

In the following problems, if a and b are real numbers, we write "$[a, b]$" to denote the closed interval $\{x \in \mathbb{R} : a \leq x \leq b\}$, and "$(a, b)$" to denote the open interval $\{x \in \mathbb{R} : a < x < b\}$.

Problem 48. ***Prove*** that if X is a set then there does not exist a one-to-one function $f : \mathcal{P}(X) \mapsto X$. □

Problem 49.

1. Let f, g be the functions defined by

   (i) $\mathrm{Dom}(f) = \mathbb{R}$,

   (ii) $f(x) = \frac{x}{\sqrt{1+x^2}}$ for $x \in \mathbb{R}$,

   (iii) $\mathrm{Dom}(g) = (-1, 1)$,

   iv) $g(y) = \frac{y}{\sqrt{1-y^2}}$ for $y \in (-1, 1)$,

   (a) ***Prove*** that $f : \mathbb{R} \mapsto (-1, 1)$, $g : (-1, 1) \mapsto \mathbb{R}$, $g \circ f = I_{\mathbf{R}}$, and $f \circ g = I_{(-1,1)}$.

   (b) ***Conclude*** from this that $\mathbb{R}$ and the open interval $(-1, 1)$ have the same cardinality.

2. If $a, b \in \mathbb{R}$ and $a < b$, let $f_{a,b}$ be the function with domain $(-1, 1)$, given by $f_{a,b}(x) = a + \frac{1}{2}(b - a)(x + 1)$ for $x \in (-1, 1)$. ***Prove*** that f is a bijection from $(-1, 1)$ to (a, b), and ***conclude*** from this that $\mathbb{R}$ and the interval (a, b) have the same cardinality.

Problem 50. ***Construct*** a bijection from the closed interval $[0, 1]$ to the open interval $(0, 1)$. (Recall that $[0, 1]$ is the set $\{x \in \mathbb{R} : 0 \leq x \leq 1\}$, and $(0, 1)$ is the set $\{x \in \mathbb{R} : 0 < x < 1\}$.)

HINT: Imagine an infinite hotel[13] H, in which

- the points of the open interval $(-1, 1)$ are the numbers of the rooms of H; each room has a number which is a member of $(0, 1)$, and for eacm member x of $(-1, 1)$ there is a room no. x. (So for example there is room no. 0.00001, room no. 0.3, room no. $\frac{1}{\pi}$, room no. $\frac{23}{77}$, room no. 0.9, room no. 0.99, room no. 0.999, etc. But of course there is no room 0 or room 1, because the rooms of H correspond to the members of the *open* interval $(0, 1)$, so 0 and 1 are not possible room numbers.)

- At some time, the hotel has a set of guests, also labeled by the members of the open interval $(0, 1)$, and each guest occupies the room with the same label (so guest no. 0.13 occupies room no. 0.13, guest no. $\frac{1}{\pi}$ occupies room no. $\frac{1}{\pi}$, and so on).

- Suddenly, two new guests, labeled 0 and 1, arrive and ask for rooms.

- And nobody, neither the old guests nor the new ones, is willing to share a room.

- So you have to accomodate these two new guests, while making sure that none of the old guests is left without a room.

If we were dealing with a finite hotel, this would be impossible. If a hotel has 100 rooms, all of which are occupied, and two new guests arrive and ask for a room, there is no way to oblige them.

But for an infinite hotel it can be done. The way you can do this is by finding within $(0, 1)$ an infinite sequence of rooms (for example, rooms $\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{4}$, $\frac{1}{5}$, $\frac{1}{6}$, and so on), and then move the guests in those rooms to other rooms also in the sequence, making room for the two new guests.

[13] This ins known as "Hilbert's holtel".