MATHEMATICS 300 — FALL 2017

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

PART V

Contents

13 An example of an application of the division theorem: sums of two squares

13.1 The quotient and the remainder

If a, b are integers, and $b \neq 0$, then the division theorem tells us that there exist unique integers q, r such that $a = bq + r$ and $0 \leq r < |b|$.

Those integers have a name.

Definition 24. Let a, b be integers such that $b \neq 0$. Let q, r be the unique integers such that $a = bq + r$ and $0 \leq r < |b|$. Then q is called the quotient of dividing a by b, and r is called the remainder of dividing a by b. □

13.2 Which integers are sums of two squares?

Which integers can be expressed as the sum of the squares of two integers? That is, for which integers n is it true that

$$(\exists x \in \mathbb{Z})(\exists y \in \mathbb{Z})x^2 + y^2 = n \quad ? \tag{13.1}$$

Clearly, the sum $x^2 + y^2$ is always nonnegative, so the only integers n for which (13.1) can possible be true are the nonnegative integers.

Furthermore, (13.1) is clearly true for $n = 0$, because $0 = 0^2 + 0^2$.

So the missing case is the one when $n \in \mathbb{N}$. And for that reason we will from now on confine our search to natural numbers n. And we will start by looking at a simple example.

13.2.1 A simple example

Problem 41. ***Prove*** *that the number* $345, 902, 753, 743$ *is not equal to the sum of two squares of integers. That is, prove that*

$$\sim (\exists x \in \mathbb{Z})(\exists y \in \mathbb{Z})x^2 + y^2 = 345, 902, 753, 743\,.$$

Solution. Suppose[1] that there exist integers x, y that satisfy the equation $x^2 + y^2 = 345, 902, 753, 743\,.$

Pick a pair (x_*, y_*) of such integers, so

$$x_* \in \mathbb{Z}\,,\ \ y_* \in \mathbb{Z}\,,\ \text{and}\ \ x_*^2 + y_*^2 = 345, 902, 753, 743\,.$$

[1] Of course, here we are starting a proof by contradiction .

Let us apply the division theorem to divide the numbers x_* and y_* by 4. The theorem tells us that we may pick integers p, q, r, s such that

$$\begin{aligned} x_* &= 4p + r\,, \\ y_* &= 4q + s\,, \\ 0 &\leq r < 4\,, \\ 0 &\leq s < 4\,. \end{aligned}$$

Since r is an integer and $0 \leq r < 4$, r must actually be equal to 0, 1, 2, or 3. Then:

$$\begin{aligned} x_r &= (4q + r)^2 \\ &= 16q^2 + 8qr + r^2 \\ &= 4(4q^2 + 2qr) + r^2\,. \end{aligned}$$

Therefore

- If $r = 0$, then $x_*^2 = 4k$, where $k = 4q^2 + 2qr = 4q^2$.
- If $r = 1$, then $x_*^2 = 4k + 1$, where $k = 4q^2 + 2qr = 4q^2 + 2q$.
- If $r = 2$, then $r^2 = 4$, so

  $$\begin{aligned} x_*^2 &= 4(4q^2 + 2qr) + 4 \\ &= 4(4q^2 + 2qr + 1) \\ &= 4(4q^2 + 4q + 1)\,, \end{aligned}$$

  so $x_*^2 = 4k$, where $k = 4q^2 + 4q + 1$.
- If $r = 3$, then $r^2 = 9$, so

  $$\begin{aligned} x_*^2 &= 4(4q^2 + 2qr) + 9 \\ &= 4(4q^2 + 2qr) + 8 + 1 \\ &= 4(4q^2 + 2qr + 2) + 1 \\ &= 4(4q^2 + 6q + 2) + 1\,, \end{aligned}$$

  so $x_*^2 = 4k + 1$, where $k = 4q^2 + 6q + 2$.

So we see that in all four cases ($r = 0$, $r = 1$, $r = 2$, $r = 3$) we have

$$x_*^2 = 4k + \rho\,, \quad \text{where } k \in \mathbb{Z} \text{ and } \rho = 0 \vee \rho = 1\,. \tag{13.2}$$

Similarly,

$$y_*^2 = 4\ell + \sigma\,, \quad \text{where } \ell \in \mathbb{Z} \text{ and } \sigma = 0 \vee \sigma = 1\,. \tag{13.3}$$

Therefore $x_*^2 + y_*^2 = 4(k + \ell) + \rho + \sigma$, and $\rho + \sigma$ can be equal to $0, 1$, or 2.

That is,

$$x_*^2 + y_*^2 = 4j + \tau\,, \quad \text{where } j \in \mathbb{Z} \text{ and } \tau = 0 \vee \tau = 1 \vee \tau = 2\,. \tag{13.4}$$

In other words, ***the remainder of dividing*** $x_*^2 + y_*^2$ ***by*** 4 ***is either*** 0***,*** 1***, or*** 2.

On the other hand, the remainder of dividing $345, 902, 753, 743$ by 4 is clearly 3, because $345, 902, 753, 740$ is divisible by 4.

It follows that $x_*^2 + y_*^2$ cannot be equal to $345, 902, 753, 743$. □

Remark 15. In the solution of Problem 41, ***the key point was the uniqueness part of the division theorem***. Indeed, we proved that the number $345, 902, 753, 743$, divided by 4, yields a quotient m that we don't care about, and a remainder of 3. If it was also possible to divide the same number by 4 with a different remainder, then there would be no contradiction between the facts that (i) the remainder of dividing $x_*^2 + y_*^2$ by 4 is either 0, 1, or 2, and (ii) $x_*^2 + y_*^2 = 345, 902, 753, 743$.

What makes our argument work is that it is ***not*** possible to divide the same number by 4 with a different remainder. And this is so because of the uniqueness of the quotient and the remainder. □

Remark 16. In the argument that we used to solve Problem 41, the only thing that mattered about the number $345, 902, 753, 743$ was that the remainder of dividing it by 4 is 3.

So, in fact, using exactly the same argument as in Problem 41, we have proved the following result.

Theorem 48. *If a natural number n is such that $n = 4k+3$ for some integer k, then it is not possible to express n as the sum of two squares of integers.*

Problem 42. ***Prove*** *that if n is a natural number such that $n = 8k + r$ for some integers k, r such that $r = 3$ or $r = 6$ or $r = 7$, then n cannot be expressed as the sum of the squares of two integers. (NOTE: If $r = 3$ then $n = 4(2k) + 3$. and if $r = 7$ then $n = 4(2k + 1) + 3$, so in these two cases the fact that n is not the sum of two squares follows from Theorem 48. So the new case here is the one corresponding to $r = 6$. The result of this problem would tell you, for example, that numbers such as 46 and 126 cannot be expressed as the sum of two squares.)* □

13.2.2 Which prime numbers are sums of two squares?

Natural numbers are products of prime numbers[2]. So maybe in order to figure out how to solve the problem of representing a natural number as a sum of two squares we can divide the problem into two steps.

1. See what happens when n is a prime number.
2. See what happens when you multiply two numbers that are sums of two squares.

Let us look at the first question. First of all, here is a fact that is easy to prove.

Theorem 49. *Every prime number which is different from 2 is odd.*

Proof. **YOU DO THIS ONE.**

Problem 43. ***Prove*** *Theorem 49.*

What is a prime number?

Definition 25. A prime number is a natural number p such that

1. $p > 1$,
2. The only natural numbers that divide p are 1 and p. □

[2] We haven't proved that yet, but we will, very soon

In view of Theorem 49, the prime numbers are all od, except for the number 2. So if p is a prime number and $p \neq 2$, then the remainder r of dividing p by 4 must be 1 or 3, because if r was 0 or 2 then p would be even.

In order words, the prime numbers other than 2 are of two kinds:

(I) Primes that are of the form $4q+1$, for an integer q,

(II) Primes that are of the form $4q+3$, for an integer q.

For the primes p of the form $4q+3$, we already know that the answer is "no, p cannot be written as the sum of two squares", because of Theorem 48

Let us look at all the primes p in order, starting with $p = 2$, and let us ask in each case whether p is or is not a sum of two squares.

- If $p = 2$, then the answer is "yes", because $2 = 1 + 1 = 1^2 + 1^2$.
- If $p = 3$, then the answer is "no", because of Theorem 48.
- If $p = 5$, then the answer is "yes", because $5 = 4 + 1 = 2^2 + 1^2$.
- If $p = 7$, then the answer is "no", because of Theorem 48.
- If $p = 11$, then the answer is "no", because of Theorem 48.
- If $p = 13$, then the answer is "yes", because $13 = 9 + 4 = 3^2 + 2^2$.
- If $p = 17$, then the answer is "yes", because $17 = 16 + 1 = 4^2 + 1^2$.
- If $p = 19$, then the answer is "no", because of Theorem 48.
- If $p = 23$, then the answer is "no", because of Theorem 48.
- If $p = 29$, then the answer is "yes", because $29 = 25 + 4 = 5^2 + 2^2$.
- If $p = 31$, then the answer is "no", because of Theorem 48.
- If $p = 37$, then the answer is "yes", because $37 = 36 + 1 = 6^2 + 1^2$.
- If $p = 41$, then the answer is "yes", because $41 = 25 + 16 = 5^2 + 4^2$.
- If $p = 43$, then the answer is "no", because of Theorem 48.
- If $p = 47$, then the answer is "no", because of Theorem 48.

- If $p = 53$, then the answer is “yes”, because $53 = 49 + 4 = 7^2 + 2^2$.
- If $p = 59$, then the answer is “no”, because of Theorem 48.
- If $p = 61$, then the answer is “yes”, because $61 = 36 + 25 = 6^2 + 5^2$.
- If $p = 67$, then the answer is “no”, because of Theorem 48.
- If $p = 71$, then the answer is “no”, because of Theorem 48.
- If $p = 73$, then the answer is “yes”, because $73 = 64 + 9 = 8^2 + 3^2$.
- If $p = 79$, then the answer is “no”, because of Theorem 48.
- If $p = 83$, then the answer is “no”, because of Theorem 48.
- If $p = 89$, then the answer is “yes”, because $89 = 64 + 25 = 8^2 + 5^2$.
- If $p = 97$, then the answer is “yes”, because $97 = 81 + 16 = 9^2 + 4^2$.
- If $p = 101$, then the answer is “yes”, because $101 = 100 + 1 = 10^2 + 1^2$.

So it would appear that all the primes of the form $4k + 1$ are sums of two squares. In fact, this is true for the first 12 such primes.

At this point, students will be tempted to say something like “it is clear that every prime of the form $4k + 1$ is the sum of two squares”.

But this is not necessarily so!

13.2.3 You cannot prove a universal statement by giving examples

Just because a universal statement $(\forall n \in \mathbb{N})P(n)$ ***is true for a few examples, it doesn’t mean that it is true in general!***

Even if the statement is true for 12 examples, or 50, or 10 million, that still does not prove that it is true in general.
Look, for example, at Problem 35. The statement that “$n^2 + n + 41$ is prime” is true for $n = 1$, $n = 2$, $n = 3$, $n = 4$, and so on. Actually, it is true for all n up to $n = 39$. That is, the statement is true for 39 examples, namely, for the first 39 natural numbers. And yet, the statement is not true for all n.

Problem 44. ***Write*** *a sentence* $P(n)$ *about a variable natural number* n*, such that*

1. $P(n)$ *is true for the first* 10^{10} *(i.e.,* $10,000,000,000$*) natural numbers* n*,*
2. $(\forall n \in \mathbb{N})P(n)$ *is not true.* □

13.2.4 One way con men exploit the gullibility of people

A standard error that people make when they think is precisely to believe that a few examples can prove a general statement.

The fact that people often make this mistake is exploited by con men, tricksters, and liars of various sorts, to persuade people of the truth of some universal statement by presenting a few examples. The trickster who does that knows that people are gullible, and will accept a few stories and a few examples as proof.

For example, a politician who wants to incite people to hate immigrants, may appear at a political convention and bring with him some people who have had a close relative or friend killed by an immigrant, and present these people to the audience. He knows that the audience is gullible, and will draw the conclusion that "immigrants are murderers". In reality, all the politician has done is prove that a few immigrants have committed crimes. Had he wanted instead to persuade his audience that Americans are criminals, he could have chosen to present examples of victims of crimes committed by Americans[3].

Math 300 students should not be gullible:

You must never accept as valid a proof based on a few examples.
And you must never submit such a proof as part of your work and claim that you actually have a proof.

[3] And he would have had a lot to choose from: Charles Manson, Ted Bundy, Timothy McVeigh, Adam Lanza, Dylan Roof, ... I'ts a very long list!

13.2.5 A surprising fact

Now let us return to the study of primes that are sums of two squares.

What we have seen is that:

- Primes of the form $4k+3$ are ***not*** sums of two squares. (This is so not because we have seen that it is so in lots of examples. It is so because we have ***proved*** it, in Theorem 48.)
- It appears to be the case that primes of the form $4k+1$ ***are*** sums of two squares, but the examples we have given so far do not prove it.

It turns out, quite remarkably, that it is indeed true that ***every prime number which is not of the form***[4] $4k+3$ ***is the sum of two squares of integers.***

This result was first published by Albert Girard in 1625, and for that reason it is sometimes know as "Girard's Theorem". Later, Fermat stated a more detailed version in 1640, but did not give a proof. The first real proof was given by Euler in 1747.

But this is a hard theorem. The proof belongs in an elementary number theory course, and is a little bit too complicated to be given in this course.

13.2.6 Another surprising fact

And here is another surprising fact:

Theorem 50. *The product of two natural numbers that are sums of two squares of integers is a sum of squares of two integers. That is*

$$(\forall a,b\in\mathbb{N})\Bigg[\bigg(\Big((\exists u,v\in\mathbb{Z})a=u^2+v^2\Big)\wedge\Big((\exists u,v\in\mathbb{Z})b=u^2+v^2\Big)\bigg)$$
$$\Longrightarrow (\exists u,v\in\mathbb{Z})ab=u^2+v^2\Bigg]. \qquad (13.5)$$

Proof.

Let a,b be arbitrary integers.

[4] That means, every prime number which is either 2 or of the form $4k+1$.

Assume that a and b are sums of two squares of integers.

Pick integers u, v such that $u^2 + v^2 = a$.

Pick integers x, y such that $x^2 + y^2 = b$. [Here, and in the previous step, I am applying Rule $\exists_{use}$, the rule for using existential sentences. This rule tells me that if $(\exists x)P(x)$, then I can pick one such x and give it a name, but *the name cannot be something that is already the name of something else.* That is why in the second step I cannot call the integeres I pick "u" and "v", because "u" and "v" are already the names of the two integers that I picked in the previous step.]

Let $m = ux - vy$, and let $n = uy + vx$.

Then m and n are integers.

Furthermore,

$$\begin{aligned}
m^2 + n^2 &= (ux - vy)^2 + (uy + vx)^2 \\
&= u^2x^2 + v^2y^2 - 2uxvy + u^2y^2 + v^2x^2 + 2uyvx \\
&= u^2x^2 + v^2y^2 + u^2y^2 + v^2x^2 \\
&= u^2x^2 + u^2y^2 + v^2y^2 + v^2x^2 \\
&= u^2(x^2 + y^2) + v^2(y^2 + x^2) \\
&= u^2b + v^2b \\
&= (u^2 + v^2)b \\
&= ab\,.
\end{aligned}$$

So ab is the sum of two squares.

Hence we have proved that "if a and b are the sum of two squares, then ab is the sum of two squares". (Rule $\Longrightarrow_{prove}$.)

And this was proved for arbitrary integers a, b. So we have proved (13.5), thanks to Rule $\forall_{prove}$. **Q.E.D.**

13.3 So, finally, which natural numbers are sums of two squares?

Let us put together all the facts we know so far.

- We know (though we haven't proved it) that every prime number that is not of the form $4k+3$ is the sum of two squares.

- We know that the product of two sums of two squares is a sum of two squares.

- And there is, in addition, a very simple fact: if we take a number a that is a sum of two squares and multiply it by a square, then the result is the sum of two squares. (Reason: Suppose $a = u^2 + v^2$. Let b be another integer. Then $ab^2 = b^2(u^2 + v^2) = (bu)^2 + (bv)^2$, so ab^2 is also the sum of two squares.

- And we know (and will prove soon) that vevery natural nmber greater than 1 is a product of primes.

If we combine all these facts, we get the following. Suppose a is a natural number and

$$a = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$$

where $p_1, p_2, \ldots, p_n$ are distinct primes.

Suppose that for all the primes p_j that are of the form $k+3$ the corresponding exponet k_j is even. Then a is the sum of two squares.

And, remarkably, these numbers are exactly those that are sums of two squares. That is, if a is a sum of two squares, then the exponents k_j corresponding to the primes p_j of the form $4k+3$ must be even.

This compleetly solves the problem if determining which natural numbers are sums of two squares although, as I said, the proof of these results is too hard for this course. But the point I wanted to make is this: ***the fact that gace us the first clue about the solution was our simple application of the division theorem.*** Naturally, a lot of work is needed after that, but the division theorem by itself has shown itself to be a very powerful tool

13.4 Some problems

Problem 45. ***Prove*** *that*

1. *If p is a prime number then one and only one of the following three possibilities occurs:*

   (a) $p = 2$,

(b) $p = 4k + 1$ *for some* $k \in \mathbb{N}$,

(c) $p = 4k + 3$ *for some* $k \in \mathbb{N}$.

2. *If* p *is a prime number then one and only one of the following four possibilties occurs:*

   (a) $p = 2$,

   (b) $p = 3$,

   (c) $p = 6k + 1$ *for some* $k \in \mathbb{Z}$,

   (d) $p = 6k + 5$ *for some* $k \in \mathbb{Z}$.

Problem 46. ***Prove*** *by induction that if* $n \in \mathbb{N}$, $a_1, a_2, \ldots, a_n$ *are integers,* $j \in \mathbb{N}$, *and* $1 \leq j \leq n$, *then* a_j *divides the product* $\prod_{k=1}^{n} a_k$. □

Problem 47. *Euclid's lemma says that if* p *is a prime number and* a, b *are integers such that* p *divides* ab, *then* p *divides* a *or* p *divides* b.

Using Euclid's Lemma, ***prove*** *by induction the following statement:*

(*) *If* p *is a prime number,* n *is a natural number, and* $a_1, a_2, \ldots, a_n$ *are integers such that* p *divides the product* $\prod_{j=1}^{n} a_j$, *then* p *divides one of the factors, that is,* $(\exists j \in \mathbb{N})(j \leq n \wedge p | a_j)$.

Problem 48. *If* $n \in \mathbb{N}$, $k \in \mathbb{Z}$, *and* $0 \leq k \leq n$, *then the* *binomial coefficient* $\binom{n}{k}$ *is defined as follows:*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \quad .$$

1. **Prove** *that, if* $n \in \mathbb{N}$, $k \in \mathbb{Z}$, *and* $1 \leq k \leq n$, *then*
$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k} .$$

2. *Using the result of Part 1,* ***prove*** *by induction that* $\binom{n}{k}$ *is an integer for every* $n \in \mathbb{N}$ *and every* $k \in \mathbb{Z}$ *such that* $0 \leq k \leq n$.

Be careful about how you choose the sentence $P(n)$ ***that you will use for the induction****. It cannot be something like "*$\binom{n}{k}$ *is an integer", because this sentence has* k, *as well as* n, *as an open variable, and that is not premitted. So* k *has to be quatified somehow.*

NOTE: It is not at all obvious that $\binom{n}{k}$ *is an integer. The number* $\binom{n}{k}$ *is defined as a quotient of two integers, and such a quotient need not be an integer.* □

14 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 numebr?", 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.

14.1 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.

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. ***Flocka 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 band". 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 we say things like

   The jurors ***find*** the defendant guilty

   or

   The jury ***finds*** the defendant guilty.

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

5. ***The sets*** $\mathbb{N}$***,*** $\mathbb{Z}$***, 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"), $\mathbb{R}$ ("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 real numbers form a complete ordered field,

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

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

Notice that "the natural numbers", "the integers", and "the real numbers" have become single objecta, "$\mathbb{N}$". "$\mathbb{Z}$". "$\mathbb{R}$". 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.*

14.1.1 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.)

14.1.2 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.
- 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[5].

14.1.3 Terms and sentences with variables: a review

In mathematical writing, there are two kinds of meaningful phrases[6], namely, ***terms*** and ***sentences***.

- 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.[7]
- 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 17. Terms are basically the same as "noun phrases", that is, phrases that can serve as the subject of an "is" sentence. So, for example,

[5] 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.

[6] 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 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.

[7] 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.

- 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.

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 42. 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 43. 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 44. 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 45. 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.. □

14.1.4 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 18. 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 $C(x)$ whatsoever and form the ser $\{x : C(x)\}$, we will have to adopt a "sophisticated" axiom in which nto all sentences are permitted. □

14.1.5 The membership criterion

Suppose we use the sentence "x is a cow", to form a set S, so

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

that is, S is "the set of all x such that x is a cow", or, in much better English, S ***is the set of all cows.***

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.

14.1.6 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

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

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

Example 46. 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

$$S = \{x \in \mathbb{N} : (\exists m \in \mathbb{N})(\exists n \in \mathbb{N})x = m^2 + n^2\}\,, \tag{14.6}$$

(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, we know that a number that is of the form $k + 3$, $k \in \mathbb{Z}$, is not the sum of two squares. And 7 is of the form $k + 3$, because $7 = 4 + 3$. So $x \notin S$. □

14.1.7 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 19. 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", "pick an a in S", is fine. □

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

14.2 When are two sets equal?

As we have explained, sets have ***members***. And, even more imprtantly, ***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

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

And, in formal language,

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

Example 47. 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 $(\forall x)(x \in A \Longleftrightarrow x \in B)$.

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

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

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

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

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

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

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.**

Example 48. 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 $(\forall x)(x \in A \Longleftrightarrow x \in B)$.

Suppose[8] $(\forall x)(x \in A \Longleftrightarrow x \in B)$.

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

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 $0 \in A \Longleftrightarrow 0 \in B$.

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

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

Example 49. Let $A = \{n \in \mathbb{R} : 6|n\}$, 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 $(\forall x)(x \in A \Longleftrightarrow x \in B)$.

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

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

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

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 $x = 6k$.

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 $x \in B$.

[8] A proof by contradiction , of course.

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 49. *Let*

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

Prove or disprove *each of the following:*

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

14.2.1 Subsets

Definition 26. Let A, B be sets. We say that A is a <u>subset</u> 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 50. The following are true:

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

Example 51.

The following are true:

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

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 subzset of B if ....

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

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

Problem 50. ***Prove*** *the four statements of Example 51.*

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 51. ***Prove*** *that the binary relation "*$\subseteq$*" is reflexive, antisymmetric, and transitive. (In the definition of these properties given in the notes, a set* S *is mentioned. Here you may think of* S *as "the set of all sets", which means that you can forget about* S*. Then, for example, the property that "*$\subseteq$*" is antisymmetric means "*$(\forall A)(\forall B)\Big((A \subseteq B \wedge B \subseteq A) \Longrightarrow A = B\Big)$*".)*

14.2.2 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 51. *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[9] 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.**

14.2.3 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:

[9] A proof by contradiction !.

Theorem 52. *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[10] 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 51 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.**

14.2.4 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.

[10] A proof by contradiction !

Definition 27. 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 28. Let a, b be any two objects. Then the unordered pair of a and b is the set $\{a, b\}$ given by

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

Remark 20. ***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. □

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

Definition 29. 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 30. 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

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

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 52. 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? And what if you do not know the names of all those presidents?

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

Let

$$B = \Big\{ x : (\exists j \in \mathbb{N})(j \le 30 \wedge x = p_j) \Big\},$$

where, for each $j \in \mathbb{N}$, 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 A. 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 $j \le 30$ and x is the j-th U.S. president. And that's exactly what we want! □

Problem 52. *How many members does the set B of Example 52 have?*

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

Problem 54. *Write a definition, in the style of Example 52, of the set X whose members are the first 325 prime numbers p such that $p - 3$ is divisible by 4.* □