Introduction to mathematical arguments

(background handout for courses requiring proofs)

by Michael Hutchings

A mathematical **proof** is an argument which convinces other people that something is true. Math isn't a court of law, so a "preponderance of the evidence" or "beyond any reasonable doubt" isn't good enough. In principle we try to prove things beyond any doubt at all — although in real life people make mistakes, and total rigor can be impractical for large projects. (There are also some subtleties in the foundations of mathematics, such as Gödel's theorem, but never mind.)

Anyway, there is a certain vocabulary and grammar that underlies all mathematical proofs. The vocabulary includes logical words such as 'or', 'if', etc. These words have very precise meanings in mathematics which can differ slightly from everyday usage. By "grammar", I mean that there are certain common-sense principles of logic, or proof techniques, which you can use to start with statements which you know and deduce statements which you didn't know before.

These notes give a very basic introduction to the above. One could easily write a whole book on this topic; see for example *How to read and do proofs: an introduction to mathematical thought process* by D. Solow). There are many more beautiful examples of proofs that I would like to show you; but this might then turn into an introduction to all the math I know. So I have tried to keep this introduction brief and I hope it will be a useful guide.

In §1 we introduce the basic vocabulary for mathematical statements. In §2 and §3 we introduce the basic principles for proving statements. We provide a handy chart which summarizes the meaning and basic ways to prove any type of statement. This chart does not include uniqueness proofs and proof by induction, which are explained in §3.3 and §4. Apendix A reviews some terminology from set theory which we will use and gives some more (not terribly interesting) examples of proofs.

The following was selected and cobbled together from piles of old notes, so it is a bit uneven; and the figures are missing, sorry. If you find any mistakes or have any suggestions for improvement please let me know.

1 Statements and logical operations

In mathematics, we study **statements**, sentences that are either true or false but not both. For example,

6 is an even integer

and

4 is an odd integer

are statements. (The first one is true, and the second is false.) We will use letters such as 'p' and 'q' to denote statements.

1.1 Logical operations

In arithmetic, we can combine or modify numbers with operations such as '$+$', '$\times$', etc. Likewise, in logic, we have certain operations for combining or modifying statements; some of these operations are 'and', 'or', 'not', and 'if...then'. In mathematics, these words have precise meanings, which are given below. In some cases, the mathematical meanings of these words differ slightly from, or are more precise than, common English usage.

Not. The simplest logical operation is 'not'. If p is a statement, then 'not p' is defined to be

- true, when p is false;
- false, when p is true.

The statement 'not p' is called the **negation** of p.

And. If p and q are two statements, then the statement 'p and q' is defined to be

- true, when p and q are both true;
- false, when p is false or q is false or both p and q are false.

Or. If p and q are two statements, then the statement 'p or q' is defined to be

- true, when p is true or q is true or both p and q are true;
- false, when both p and q are false.

In English, sometimes "p or q" means that p is true or q is true, but not both. However, this is *never* the case in mathematics. We always allow for the possibility that both p and q are true, unless we explicitly say otherwise.

If... then. If p and q are statements, then the statement 'if p then q' is defined to be

- true, when p and q are both true or p is false;
- false, when p is true and q is false.

We sometimes abbreviate the statement 'if p then q' by 'p implies q', or '$p \Rightarrow q$'. If p is false, then we say that $p \Rightarrow q$ is **vacuously true**.

If and only if. If p and q are statements, then the statement 'p if and only if q' is defined to be

- true, when p and q are both true or both false;
- false, when one of p, q is true and the other is false.

The symbol for 'if and only if' is '$\iff$'. When $p \iff q$ is true, we say that p and q are **equivalent**.

1.2 Quantifiers

Consider the sentence

x is even.

This is not what we have been calling a statement; we can't say whether it is true or false, because we don't know what x is.

There are three basic ways to turn this sentence into a statement. The first is to say exactly what x is:

When $x = 6$, x is even.

The following are two more interesting ways of turning the sentence into a statement:

For every integer x, x is even.

There exists an integer x such that x is even.

The phrases 'for every' and 'there exists' are called **quantifiers**.

As an example of the use of quantifiers, we can give precise definitions of the terms 'even' and 'odd'.

Definition. An integer x is **even** if there exists an integer y such that $x = 2y$.

(The 'if' in this definition is really an 'if and only if'. Mathematical literature tends to misuse the word 'if' this way when making definitions, and we will do this too.)

Definition. An integer x is **odd** if there exists an integer y such that $x = 2y + 1$.

Notation for quantifiers. We will call a sentence such as 'x is even' that depends on the value of x a "statement about x". We can denote the sentence 'x is even' by '$P(x)$'; then $P(5)$ is the statement '5 is even', $P(72)$ is the statement '72 is even', and so forth.

If S is a set and $P(x)$ is a statement about x, then the notation

$$(\forall x \in S)\ P(x)$$

means that $P(x)$ is true for every x in the set S. (See Appendix A for a discussion of sets.) The notation

$$(\exists x \in S)\ P(x)$$

means that there exists at least one element x of S for which $P(x)$ is true.

We denote the set of integers by '$\mathbb{Z}$'. Using the above notation, the definition of 'x is even' given previously becomes

$$(\exists y \in \mathbb{Z})\ x = 2y.$$

Of course, this is still a statement about x. We can turn this into a statement by using a quantifier to say what x is. For instance, the statement

$$(\forall x \in \mathbb{Z})\,(\exists y \in \mathbb{Z})\; x = 2y$$

says that all integers are even. (This is false.) The statement

$$(\exists x \in \mathbb{Z})\,(\exists y \in \mathbb{Z})\; x = 2y$$

says that there exists at least one even integer. (This is true.)

The sentence

$$(\exists y \in \mathbb{Z})\; x = 2y + 1$$

means that x is odd. The statement

$$(\forall x \in \mathbb{Z})\,\Big((\exists y \in \mathbb{Z})\; x = 2y\Big) \text{ or } \Big((\exists y \in \mathbb{Z})\; x = 2y + 1\Big)$$

says that every integer is even or odd.

The *order* of quantifiers is very important; changing the order of the quantifiers in a statement will often change the meaning of a statement. For example, the statement

$$(\forall x \in \mathbb{Z})\,(\exists y \in \mathbb{Z})\; x < y$$

is true. However the statement

$$(\exists y \in \mathbb{Z})\,(\forall x \in \mathbb{Z})\; x < y$$

is false.

1.3 How to negate statements.

We often need to find the negations of complicated statements. How do you *deny* that something is true? The rules for doing this are given in the right-hand column of Table 1.

For example, suppose we want to negate the statement

$$(\forall x \in \mathbb{Z})\,\Big((\exists y \in \mathbb{Z})\; x = 3y + 1\Big) \Rightarrow \Big((\exists y \in \mathbb{Z})\; x^2 = 3y + 1\Big).$$

First, we put a 'not' in front of it:

$$\text{not } (\forall x \in \mathbb{Z})\,\Big((\exists y \in \mathbb{Z})\; x = 3y + 1\Big) \Rightarrow \Big((\exists y \in \mathbb{Z})\; x^2 = 3y + 1\Big).$$

Using the rule for negating a 'for every' statement, we get

$$(\exists x \in \mathbb{Z}) \text{ not } \left(\Big((\exists y \in \mathbb{Z})\, x = 3y + 1 \Big) \Rightarrow \Big((\exists y \in \mathbb{Z})\, x^2 = 3y + 1 \Big) \right).$$

Using the rule for negating an 'if...then' statement, we get

$$(\exists x \in \mathbb{Z}) \Big((\exists y \in \mathbb{Z})\, x = 3y + 1 \Big) \text{ and not } (\exists y \in \mathbb{Z})\, x^2 = 3y + 1.$$

Using the rule for negating a 'there exists' statement, we get

$$(\exists x \in \mathbb{Z}) \Big((\exists y \in \mathbb{Z})\, x = 3y + 1 \Big) \text{ and } (\forall y \in \mathbb{Z})\, x^2 \neq 3y + 1.$$

2 How to prove things

Let us start with a silly example. Consider the following conversation between mathematicians Alpha and Beta.

ALPHA: I've just discovered a new mathematical truth!

BETA: Oh really? What's that?

ALPHA: For every integer x, if x is even, then x^2 is even.

BETA: Hmm... are you sure that this is true?

ALPHA: Well, isn't it obvious?

BETA: No, not to me.

ALPHA: OK, I'll tell you what. You give me any integer x, and I'll show you that the sentence 'if x is even, then x^2 is even' is true. *Challenge* me.

BETA (eyes narrowing to slits): All right, how about $x = 17$.

ALPHA: That's easy. 17 is not even, so the statement 'if 17 is even, then 17^2 is even' is vacuously true. Give me a harder one.

BETA: OK, try $x = 62$.

ALPHA: Since 62 is even, I guess I have to show you that 62^2 is even.

BETA: That's right.

ALPHA (counting on her fingers furiously): According to my calculations, $62^2 = 3844$, and 3844 is clearly even...

BETA: Hold on. It's not so clear to me that 3844 is even. The definition says that 3844 is even if there exists an integer y such that $3844 = 2y$. If you want to go around saying that 3844 is even, you have to *produce* an integer y that works.

ALPHA: How about $y = 1922$.

BETA: Yes, you have a point there. So you've shown that the sentence 'if x is even, then x^2 is even' is true when $x = 17$ and when $x = 62$. But there are *billions* of integers that x could be. How do you know you can do this for every one?

ALPHA: Let x be any integer.

BETA: Which integer?

ALPHA: Any integer at all. It doesn't matter which one. I'm going to show you, using only the fact that x is an integer and nothing else, that if x is even then x^2 is even.

BETA: All right...go on.

ALPHA: So suppose x is even.

BETA: But what if it isn't?

ALPHA: If x isn't even, then the statement 'if x is even, then x^2 is even' is vacuously true. The only time I have anything to worry about is when x is even.

BETA: OK, so what do you do when x is even?

ALPHA: By the definition of 'even', we know that there exists at least one integer y such that $x = 2y$.

BETA: Only one, actually.

ALPHA: I think so. Anyway, let y be an integer such that $x = 2y$. Squaring both sides of this equation, we get $x^2 = 4y^2$. Now to prove that x^2 is even, I have to exhibit an integer, twice which is x^2.

BETA: Doesn't $2y^2$ work?

ALPHA: Yes, it does. So we're done.

BETA: And since you haven't said anything about what x is, except that it's an integer, you know that this will work for any integer at all.

ALPHA: Right.

BETA: OK, I understand now.

ALPHA: So here's another mathematical truth. For every integer x, if x is odd, then x^2 is...

This dialogue illustrates several important points. First, a **proof** is an explanation which convinces other mathematicians that a statement is true. A good proof also helps them *understand* why it is true. The dialogue also illustrates several of the basic techniques for proving that statements are true.

Table 1 summarizes just about everything you need to know about logic. It lists the basic ways to prove, use, and negate every type of statement. In boxes with multiple items, the first item listed is the one most commonly used. Don't worry if some of the entries in the table appear cryptic at first; they will make sense after you have seen some examples.

In our first example, we will illustrate how to prove 'for every' statements and 'if...then' statements, and how to use 'there exists' statements. These ideas have already been introduced in the dialogue.

Example. Write a proof that for every integer x, if x is odd, then $x + 1$ is even.

This is a 'for every' statement, so the first thing we do is write

> Let x be any integer.

We have to show, using only the fact that x is an integer, that if x is odd then $x + 1$ is even. So we write

> Suppose x is odd.

We must somehow use this assumption to deduce that $x + 1$ is even. Recall that the statement 'x is odd' means that there exists an integer y such that $x = 2y + 1$. Also, we can give this integer y any name we like; so to avoid confusion below, we are going to call it 'w'. So to use the assumption that x is odd, we write

Statement	Ways to Prove it	Ways to Use it	How to Negate it
p	• Prove that p is true. • Assume p is false, and derive a contradiction.	• p is true. • If p is false, you have a contradiction.	not p
p and q	• Prove p, and then prove q.	• p is true. • q is true.	(not p) or (not q)
p or q	• Assume p is false, and deduce that q is true. • Assume q is false, and deduce that p is true. • Prove that p is true. • Prove that q is true.	• If $p \Rightarrow r$ and $q \Rightarrow r$ then r is true. • If p is false, then q is true. • If q is false, then p is true.	(not p) and (not q)
$p \Rightarrow q$	• Assume p is true, and deduce that q is true. • Assume q is false, and deduce that p is false.	• If p is true, then q is true. • If q is false, then p is false.	p and (not q)
$p \iff q$	• Prove $p \Rightarrow q$, and then prove $q \Rightarrow p$. • Prove p and q. • Prove (not p) and (not q).	• Statements p and q are interchangeable.	(p and (not q)) or ((not p) and q)
$(\exists x \in S)\ P(x)$	• Find an x in S for which $P(x)$ is true.	• Say "let x be an element of S such that $P(x)$ is true."	$(\forall x \in S)$ not $P(x)$
$(\forall x \in S)\ P(x)$	• Say "let x be any element of S." Prove that $P(x)$ is true.	• If $x \in S$, then $P(x)$ is true. • If $P(x)$ is false, then $x \notin S$.	$(\exists x \in S)$ not $P(x)$

Table 1: Logic in a nutshell.

Let w be an integer such that $x = 2w + 1$.

Now we want to prove that $x + 1$ is even, i.e., that there exists an integer y such that $x + 1 = 2y$. Here's how we do it:

Adding 1 to both sides of this equation, we get $x + 1 = 2w + 2$. Let $y = w + 1$; then y is an integer and $x + 1 = 2y$, so $x + 1$ is even.

We have completed our proof, so we can write

Q.E.D.

which stands for something in Latin which means "that which was to be shown". A common typographical convention is to draw a box instead:

$\square$

In the next example, we will illustrate the use of 'and' statements.

Example. Write a proof that for every integer x and for every integer y, if x is odd and y is odd then xy is odd.

(Note that the first 'and' in this statement is not a logical 'and'; it is just there to smooth things out when we translate the symbols

$$(\forall x \in \mathbb{Z})\,(\forall y \in \mathbb{Z})$$

into English.)

First, following the standard procedure for proving statements that begin with 'for every', we write

Let x and y be any integers.

We need to prove that if x is odd and y is odd then xy is odd. Following the standard procedure for proving 'if…then' statements, we write

Suppose x is odd and y is odd.

This is an 'and' statement. We can use it to conclude that x is odd. We can then use the statement that x is odd to give us an integer w such that $x = 2w + 1$. In our proof, we write

Since x is odd, choose an integer w such that $x = 2w + 1$.

We can also use our 'and' statement to conclude that y is odd. We write

> Since y is odd, choose an integer v such that $y = 2v + 1$.

Now we need to show that xy is odd. We can do this as follows:

> Then $xy = 4vw + 2v + 2w + 1$. Let $z = 2vw + v + w$; then $xy = 2z + 1$, so xy is odd. $\square$

Next, we will illustrate how to prove and use 'if and only if' statements. The proof of a statement of the form $p \iff q$ usually looks like this:

> ($\Rightarrow$) [proof that $p \Rightarrow q$]
>
> ($\Leftarrow$) [proof that $q \Rightarrow p$]
>
> $\square$

Example. Write a proof that for every integer x, x is even if and only if $x + 1$ is odd.

> Let x be any integer. We must show x is even if and only if $x + 1$ is odd.
>
> ($\Rightarrow$) Suppose x is even. Choose an integer y such that $x = 2y$. Then y is also an integer such that $x + 1 = 2y + 1$, so $x + 1$ is odd.
>
> ($\Leftarrow$) Suppose $x + 1$ is odd. Choose an integer y such that $x + 1 = 2y + 1$. Then y is also an integer such that $x = 2y$, so x is even. $\square$

Now we can conclude that for any integer x, the statements 'x is even' and '$x + 1$ is odd' are **interchangeable**; this means that we can take any true statement and replace some occurrences of the phrase 'x is even' with the phrase '$x + 1$ is odd' to get another true statement. For example, mathematicians Alpha and Beta proved in the dialogue that

> For every integer x, if x is even then x^2 is even

So the following is also a true statement:

> For every integer x, if $x + 1$ is odd then x^2 is even.

Remark. All the statements we are proving here about even and odd numbers can be proved more simply using some basic facts about mod 2 arithmetic. However our aim here is to illustrate the fundamental rules of mathematical proofs by giving unusually detailed proofs of some facts which you probably already know.

Exercises.

1. Prove the following statements:

   (a) For every integer x, if x is even, then for every integer y, xy is even.

   (b) For every integer x and for every integer y, if x is odd and y is odd then $x + y$ is even.

   (c) For every integer x, if x is odd then x^3 is odd.

   What is the negation of each of these statements?

2. Prove that for every integer x, $x + 4$ is odd if and only if $x + 7$ is even.

3. Figure out whether the statement we negated in §1.3 is true or false, and prove it (or its negation).

4. Prove that for every integer x, if x is odd then there exists an integer y such that $x^2 = 8y + 1$.

3 More proof techniques

3.1 Proof by cases

We will consider next how to make use of 'or' statements. The first entry in the box in the table is what we call "proof by cases". This is best explained by an example.

Example. For every integer x, the integer $x(x + 1)$ is even.

Proof. Let x be any integer. Then x is even or x is odd. (Some people might consider this too obvious to require a proof, but a proof can be given using the Division Theorem, see §4.2, which here tells us that every integer can be divided by 2 with a remainder of 0 or 1.) We will prove that in both of these cases, $x(x+1)$ is even.

Case 1: suppose x is even. Choose an integer k such that $x = 2k$. Then $x(x+1) = 2k(2k+1)$. Let $y = k(2k+1)$; then y is an integer and $x(x+1) = 2y$, so $x(x+1)$ is even.

Case 2: suppose x is odd. Choose an integer k such that $x = 2k+1$. Then $x(x+1) = (2k+1)(2k+2)$. Let $y = (2k+1)(k+1)$; then $x(x+1) = 2y$, so $x(x+1)$ is even. $\square$

3.2 Proof by contradiction

Notice that near the top of the chart, we mention that one can prove a statement by assuming that it is false and deducing a contradiction. This is a useful and fun technique called "proof by contradiction".

Here is how it works. Suppose that we want to prove that the statement P is true. We begin by assuming that P is false. We then try to deduce a **contradiction**, i.e. some statement Q which we know is false. If we succeed, then our assumption that P is false must be wrong! So P is true, and our proof is finshed.

We will give two examples involving rational numbers. Recall that a real number x is **rational** if there exist integers p and q with $q \neq 0$ such that $x = p/q$. If x is not rational it is called **irrational**.

Example. Prove that if x is rational and y is irrational, then $x+y$ is irrational. (More precisely we should perhaps include quantifiers and say "for all rational numbers x and all irrational numbers y, the sum $x+y$ is irrational", but you know what I mean.)

Let us assume the negation of what we are trying to prove: namely that there exist a rational number x and an irrational number y such that $x+y$ is rational. We observe that

$$y = (x+y) - x.$$

Now $x+y$ and x are rational by assumption, and the difference of two rational numbers is rational (since $p/q - p'/q' = (pq' - qp')/(qq')$). Thus y is rational. But that contradicts our assumptions. So our assumptions cannot be right! So if x is rational and y is irrational then $x+y$ is irrational. $\square$

Example. Prove that $\sqrt{2}$ is irrational.

Suppose $\sqrt{2}$ is rational, i.e. $\sqrt{2} = a/b$ for some integers a and b with $b \neq 0$. We can assume that b is positive, since otherwise we can simply change the signs of both a and b. (Then a is positive too, although we will not need this.) Let us choose integers a and b with $\sqrt{2} = a/b$, such that b is positive and as small as possible. (We can do this by the Well-Ordering Principle, which says that every nonempty set of positive integers has a smallest element; see §4.2.)

Squaring both sides of the equation $\sqrt{2} = a/b$ and multiplying both sides by b^2, we obtain $a^2 = 2b^2$. Since a^2 is even, it follows that a is even. Thus $a = 2k$ for some integer k, so $a^2 = 4k^2$, and hence $b^2 = 2k^2$. Since b^2 is even, it follows that b is even. Since a and b are both even, $a/2$ and $b/2$ are integers with $b/2 > 0$, and $\sqrt{2} = (a/2)/(b/2)$, because $(a/2)/(b/2) = a/b$. But we said before that b is as small as possible, so this is a contradiction. Therefore $\sqrt{2}$ cannot be rational. □

This particular type of proof by contradiction is known as **infinite descent**, which is used to prove various theorems in classical number theory. If there exist positive integers a and b such that $a/b = \sqrt{2}$, then the above proof shows that we can find smaller positive integers a and b with the same property, and repeating this process, we will get an infinite descending sequence of positive integers, which is impossible.

Recall that in the above proof, we said

> We can assume that b is positive, since otherwise we can simply change the signs of both a and b.

Another way to write this would be

> **Without loss of generality**, $b > 0$.

"Without loss of generality" means that there are two or more cases (in this proof the cases when $b > 0$ and $b < 0$), but considering just one particular case is enough to prove the theorem, because the proof for the other case or cases works the same way.

3.3 Uniqueness proofs

Suppose we want to prove that the object x satisfying a certain property, if it exists, is *unique*. There is a standard strategy for doing this. We let x

and y be two objects both satisfying the given property, and we then try to deduce that $x = y$.

A classic example of a uniqueness proof comes from group theory. Recall that a **group** is a set G together with a rule for multiplying any two elements of G to obtain another element of G. The definition of a group requires that this multiplication is associative (though not necessarily commutative), and that there is an **identity element** $e \in G$ such that

$$(\forall x \in G) \quad ex = xe = x. \tag{1}$$

(Also any element x has an **inverse** x^{-1} such that $xx^{-1} = x^{-1}x = e$.)

Example. Prove that the identity element $e \in G$ satisfying (1) is unique.

Let e_1, e_2 be elements of G satisfying $e_1x = xe_1 = x$ and $e_2x = xe_2 = x$ for all $x \in G$. We will show that $e_1 = e_2$. The trick is to multiply e_1 and e_2 together in order to obtain an "identity crisis". Since e_1 is an identity element, we have $e_1e_2 = e_2$. But since e_2 is an identity element, we have $e_1e_2 = e_1$. Thus $e_1 = e_2$. □

Exercise. Prove that the inverse of a given element $x \in G$ is unique.

4 Proof by induction

Mathematical induction is a useful technique for proving statements about natural numbers.

4.1 The principle of mathematical induction

Let $P(n)$ be a statement about the positive integer n. For example, perhaps

$$P(n) = \text{“}n \text{ is a multiple of 5.”}$$

or

$$P(n) = \text{“If } n \text{ is even, then } n^2 \text{ is divisible by 4.”}$$

Suppose we want to show that $P(n)$ is true for every positive integer n. How can we do this? One way is to prove the following two statements:

(a) $P(1)$ is true.

(b) For every $n \in \mathbb{Z}^+$, if $P(n)$ is true, then $P(n+1)$ is true.

Why is this sufficient? Well, suppose we have proved (a) and (b) above. Then we know that $P(1)$ is true. Since $P(1) \Rightarrow P(2)$, we know that $P(2)$ is true. Since $P(2) \Rightarrow P(3)$, we know that $P(3)$ is true. Since $P(3) \Rightarrow P(4)$, we know that $P(4)$ is true. We can continue this indefinitely, so we see that $P(n)$ is true for every positive integer n.

By analogy, suppose we have a chain of dominoes standing on end. If we push over the first domino, and if each domino knocks over the next domino as it falls, then eventually every domino will fall. This reasoning is called the principle of **mathematical induction**. In fact this principle can be regarded as one of the axioms defining the natural numbers. Let us state it precisely.

Principle of Mathematical Induction (PMI). Let $P(n)$ be a statement about the positive integer n. If the following are true:

1. $P(1)$,
2. $(\forall n \in \mathbb{Z}^+)\ P(n) \Rightarrow P(n+1)$,

then $(\forall n \in \mathbb{Z}^+)\ P(n)$.

A proof by induction consists of two parts. In the first part, called the **base case**, we show that $P(1)$ is true. In the second part, called the **inductive step**, we assume that n is a positive integer such that $P(n)$ is true, (although we don't know what n is), and we deduce that $P(n+1)$ is true. The assumption that $P(n)$ is true is called the **inductive hypothesis**. (This may look like circular reasoning, but it is not! Think about the dominoes again.)

Example. For every positive integer n,

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Proof. We will use induction on n.

Base case: When $n = 1$, we have$1 + \cdots + n = 1$, and $n(n+1)/2 = 1 \cdot 2/2 = 1$.

Inductive step: Suppose that for a given $n \in \mathbb{Z}^+$,

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}. \qquad \text{(inductive hypothesis)}$$

Our goal is to show that

$$1 + 2 + \cdots + n + (n+1) = \frac{[n+1]([n+1]+1)}{2},$$

i.e.,

$$1 + 2 + \cdots + n + (n+1) = \frac{(n+1)(n+2)}{2}.$$

Adding $(n+1)$ to both sides of the inductive hypothesis, we get

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\ &= \frac{(n+2)(n+1)}{2}. \end{aligned}$$

$\square$

Recall that if a and b are real numbers and $ab = 0$, then $a = 0$ or $b = 0$. Using induction, we can extend this to the following:

Example. If $a_1, a_2, \ldots, a_n$ are real numbers and $a_1 a_2 \cdots a_n = 0$, then $a_i = 0$ for some i with $1 \leq i \leq n$.

Proof. We will use induction on n.

Base case: For $n = 1$, this is trivial.

Inductive step: Suppose the statement is true for n. We wish to show that the statement is true for $n+1$. Suppose $a_1, \ldots, a_n, a_{n+1}$ are real numbers such that $a_1 a_2 \cdots a_n a_{n+1} = 0$. Since $(a_1 \cdots a_n) a_{n+1} = 0$, it follows that $a_1 \cdots a_n = 0$ or $a_{n+1} = 0$.

If $a_1 \cdots a_n = 0$, then by inductive hypothesis, $a_i = 0$ for some i with $1 \leq i \leq n$, and we are done. If $a_{n+1} = 0$, we are also done. $\square$

In mathematical writing, simple induction proofs like this are often omitted. For example, one might write "since the product of two nonzero real numbers is nonzero, it follows by induction that the product of n nonzero real numbers is nonzero". However induction is an essential tool for breaking down more complicated arguments into simple steps.

There are many (equivalent) variants of the principle of induction. For example, one can start at 0 instead of 1, to prove that some statement is true for all nonnegative integers. One can also prove a statement about several positive integers by doing induction on one variable at a time. Another important variant is the following:

Strong induction. Let $P(n)$ be a statement about the positive integer n. Suppose that for every positive integer n,

(*) If $P(n')$ is true for all positive integers $n' < n$, then $P(n)$ is true.

Then $P(n)$ is true for all positive integers n.

Note that no base case is needed. To see this, suppose we have proved (*) for all positive integers n. Putting $n = 1$ into (*), we deduce that $P(1)$ is true, since the statement "$P(n')$ is true for all positive integers $n' < 1$" is vacuously true. Putting $n = 2$ into (*) we deduce that $P(2)$ is true. Thus $P(1)$ and $P(2)$ are true, so putting $n = 3$ into (*) we deduce that $P(3)$ is true. And so on.

To give an example of proof by strong induction, recall that an integer $p > 1$ is **prime** if it has no integer divisors other than 1 and p.

Theorem. Any integer $n > 1$ can be expressed as a product of prime numbers.

Proof. We use strong induction on n (starting at 2 instead of 1). Let $n > 1$ be an integer and suppose that every integer n' with $2 \leq n' < n$ is a product of primes. We need to show that n is a product of primes. If n is prime then n is the product of one prime number (itself) and we are done. If n is not prime then n is divisible by an integer a with $1 < a < n$, so $n = ab$ where a and b are integers with $1 < a, b < n$. By inductive hypothesis, a and b are both products of primes, and since $n = ab$, it follows that n is a product of primes. □

4.2 The Well-Ordering Principle

If S is a set of integers, then a **least element** of S is an element $x \in S$ such that $x \leq y$ for all $y \in S$. The following may seem obvious.

Well-Ordering Principle (WOP). Any nonempty set of positive integers has a least element.

However, it is not true for negative integers, rational numbers, or real numbers. For example, $\{x \in \mathbb{R} \mid x > 0\}$ has no least element.

The well-ordering principle is equivalent to the principle of mathematical induction. To see this, we will first prove that the principle of induction implies the well-ordering principle. In other words, we will prove WOP by induction.

PMI⇒WOP. Suppose **PMI** is true. We will prove **WOP**. Let S be a set of positive integers with no least element. We will show that S is empty. To do this, we will prove by induction on n that for every positive integer n, S does not contain any numbers less than n.

Base case: S cannot contain any numbers smaller than 1, since S is a set of positive integers.

Inductive step: Suppose S does not contain any numbers smaller than n. We wish to show that S does not contain any numbers smaller than $n+1$. It is enough to show that $n \notin S$. If $n \in S$, then n is a least element of S, since S contains no numbers less than n. But we assumed that S has no least element, so this is a contradiction. □

WOP⇒PMI. Suppose **WOP** is true. We will prove **PMI**. Let $P(n)$ be a statement about the positive integer n. Suppose that $P(1)$ is true, and suppose for all n, $P(n) \Rightarrow P(n+1)$. We must show that for all n, $P(n)$ is true. Suppose to the contrary that $P(n)$ is false for some n. Let

$$S := \{n \in \mathbb{Z}^+ \mid P(n) \text{ is false}\}.$$

By assumption this set is nonempty, so it contains a least element n_0. Now $n_0 \neq 1$, because we know that $P(1)$ is true. So $n_0 > 1$. Then $n_0 - 1$ is a positive integer, and since it is smaller than n_0, it is not in the set S. Thus $P(n_0 - 1)$ is true. But $P(n_0 - 1)$ implies $P(n_0)$, so $P(n_0)$ is true. Thus $n_0 \notin S$, a contradiction. $\square$

There are some variants of the well-ordering principle which are easily seen to be equivalent to it. For example any nonempty set of integers (possibly negative) with a lower bound has a least element, and any nonempty set of integers with an upper bound has a largest element. (A **lower bound** on S is a number L such that $x \geq L$ for all $x \in S$. An **upper bound** on S is a number U such that $x \leq U$ for all $x \in S$. A **largest element** of S is an element $x \in S$ such that $x \geq y$ for all $y \in S$.)

A useful application of the well-ordering principle is the following:

Division theorem. If a and b are integers with $b > 0$, then there exist unique integers q and r such that $a = qb + r$ and $0 \leq r < b$.

(The integer q is the "quotient" when a is divided by b, and r is the **remainder**. In elementary school you learned an algorithm for finding q and r. But let's now prove that they exist and are unique.)

Proof. The idea is that we want q to be the largest integer such that $a \geq qb$. So let

$$S := \{q \in \mathbb{Z} \mid a - qb \geq 0\}.$$

This set is nonempty; for example $-|a| \in S$ since $b > 0$. It also has an upper bound, since $a - qb \geq 0$ implies $q \leq |a|$. So by the well ordering principle, S contains a largest element q. Let $r = a - qb$. Then $r \geq 0$ by definition of S. Also $r < b$, or else we would have $a - (q+1)b = r - b \geq 0$, so $q + 1 \in S$, contradicting the fact that q is the largest element of S. So q and r exist.

Uniqueness is pretty easy to see; if q is any smaller then the remainder will be too big. But let us prove uniqueness using our standard strategy. Suppose $a = qb + r = q'b + r'$ with $0 \leq r, r' < b$. Subtracting we obtain $(q - q')b = r' - r$. We must have $q - q' = 0$, because there is no way to obtain a nonzero multiple of b by subtracting two elements of the set $\{0, 1, \ldots, b-1\}$, because the largest difference between any two elements of this set is $b - 1$. Since $q - q' = 0$, it follows that $r - r' = 0$ also. This proves uniqueness. $\square$

Exercises.

1. Fix a real number $x \neq 1$. Show that for every positive integer n,

$$1 + x + x^2 + \ldots + x^n = \frac{x^{n+1} - 1}{x - 1}.$$

2. Guess a formula for

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n(n+1)}$$

and prove it by induction. *Hint:* Compute the above expression for some small values of n.

3. Show that a $2^n \times 2^n$ checkerboard with one square removed can be tiled with L-triominoes. (An **L-triomino** is a shape consisting of three squares joined in an 'L'-shape.)

4. Show that the smallest element of a nonempty set of positive integers is unique.

A Sets

In this appendix we review some (but not all) basic concepts of set theory, and we give some simple examples of mathematical proofs.

A.1 Sets

Intuitively, a **set** is a collection of objects. Some commonly used sets are:

$\mathbb{R}$ = the set of real numbers,

$\mathbb{Q}$ = the set of rational numbers,

$\mathbb{Z}$ = the set of integers,

$\mathbb{N}$ = the set of natural numbers (nonnegative integers),

$\mathbb{Z}^+$ = the set of positive integers.

One can describe a set by listing, in curly braces, all the objects that the set contains. For example, the statement

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

defines S to be the set containing the numbers 1, 2, and 3. Sometimes we use an ellipsis $(\ldots)$ to save ink, especially for sets with infinitely many elements; for example,

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}.$$

The objects that a set contains are called the **elements**, or **members**, of that set. So 1 is an element of $\mathbb{N}$, while -4 is not. The notation '$x \in A$' means that x is an element of the set A. The notation '$x \notin A$' means that x is *not* an element of A. For example, $5 \in \mathbb{N}$ and $\pi \in \mathbb{R}$, while $3/2 \notin \mathbb{Z}$ and $\sqrt{2} \notin \mathbb{Q}$. (A proof of the last assertion is given in §3.2.)

The elements of a set can be other sets; for example, $\{1, \{2\}\}$ is the set whose elements are 1 and $\{2\}$. So $1 \in \{1, \{2\}\}$ and $\{2\} \in \{1, \{2\}\}$, but $2 \notin \{1, \{2\}\}$. The **empty set**, denoted $\emptyset$, is a special set which doesn't have any elements; in other words, $\emptyset = \{\}$. One can think of the empty set as a box with nothing inside.

Another way to describe a set is to give a criterion for deciding whether or not an object is an element of the set. For example, the set of natural numbers could be defined as follows:

$$(\forall x)\; x \in \mathbb{N} \Longleftrightarrow x \in \mathbb{Z} \;\text{ and }\; x \geq 0.$$

If $P(x)$ is a statement about x, we use the notation $\{x \mid P(x)\}$ to indicate the set of all x for which $P(x)$ is true. For example,

$$\mathbb{N} = \{x \mid x \in \mathbb{Z} \;\text{ and }\; x \geq 0\}.$$

Another notation for this is

$$\{x \in \mathbb{Z} \mid x \geq 0\}.$$

This reads, "the set of integers x such that $x \geq 0$." Some more examples:

$$\begin{aligned}
\mathbb{Q} &= \{x \in \mathbb{R} \mid (\exists a, b \in \mathbb{Z})\, b \neq 0 \;\text{ and }\; x = a/b\}, \\
\emptyset &= \{x \in \mathbb{Z} \mid x^2 = 3\}, \\
\{1, 2, 3\} &= \{x \in \mathbb{N} \mid x > 0 \;\text{ and }\; x < 4\} \\
\text{the set of even integers} &= \{x \in \mathbb{Z} \mid (\exists y \in \mathbb{Z})\, x = 2y\}.
\end{aligned}$$

If A and B are sets, and if every element of A is also an element of B, we say that A is a **subset** of B, and we write $A \subset B$. In symbols,

$$A \subset B \iff (\forall x)\; x \in A \Rightarrow x \in B$$

For example, $\mathbb{Z}$ is a subset of $\mathbb{R}$, but $\mathbb{R}$ is not a subset of $\mathbb{Z}$. Every set is a subset of itself. Also, the empty set is a subset of every set; for any set A, the statement

$$(\forall x)\ x \in \emptyset \Rightarrow x \in A$$

is vacuously true, since the statement "$x \in \emptyset$" is always false. On the other hand, the empty set is the only set that is a subset of the empty set.

Two sets are equal if and only if they have the same elements; in terms of subsets,

$$A = B \iff A \subset B \ \text{ and } \ B \subset A$$

For example,

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

but

$$\{1, \{2\}\} \neq \{1, 2\}.$$

A.2 Unions and intersections

The **union** of two sets A and B, denoted by $A \cup B$, is the set of all objects that are in A or B (or both):

$$A \cup B := \{x \mid x \in A \ \text{ or } \ x \in B\}.$$

The **intersection** of A and B is the set of all objects that are in both A and B:

$$A \cap B := \{x \mid x \in A \ \text{ and } \ x \in B\}.$$

For example,

$$\begin{aligned} \{1, 2, 3\} \cup \{2, 3, 4\} &= \{1, 2, 3, 4\}, \\ \{1, 2, 3\} \cap \{2, 3, 4\} &= \{2, 3\}. \end{aligned}$$

Venn diagrams provide a nice way to visualize these and other set-theoretic concepts. In Figure **??**(a), the inside of the circle on the left represents the contents of A, while the inside of the circle on the right represents B. The shaded region is $A \cup B$. In Figure **??**(b), the shaded region is $A \cap B$. How would you demonstrate the meaning of "$A \subset B$" with a Venn diagram?

The following are some basic properties of the union and intersection operations. We will leave the proofs of most of these facts as exercises.

Commutative properties.

$$A \cup B = B \cup A \qquad A \cap B = B \cap A$$

Associative properties.

$$A \cup (B \cup C) = (A \cup B) \cup C$$

$$A \cap (B \cap C) = (A \cap B) \cap C$$

Distributive properties.

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$A \cup (B \cup C) = (A \cup B) \cup (A \cup C)$$

$$A \cap (B \cap C) = (A \cap B) \cap (A \cap C)$$

Other facts.

$$A \cup A = A = A \cap A$$

$$A \cup \emptyset = A$$

$$A \cap \emptyset = \emptyset$$

$$A \cap B \subset A \subset A \cup B$$

$$A \cap B \subset B \subset A \cup B$$

A proof that two sets are equal usually consists of two parts: in the first part, labeled '($\subset$)', we show that the first set is a subset of the second; in the second part of the proof, labeled '($\supset$)', we show that the second set is a subset of the first.

Example. Prove that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

($\subset$) Suppose $x \in A \cup (B \cap C)$. We wish to show that $x \in (A \cup B) \cap (A \cup C)$. By definition of union, $x \in A$ or $x \in B \cap C$.

Case 1: Suppose $x \in A$. Then $x \in A$ or $x \in B$, so $x \in A \cup B$. Likewise, $x \in A \cup C$. Thus $x \in A \cup B$ and $x \in A \cup C$, so $x \in (A \cup B) \cap (A \cup C)$.

Case 2: Suppose $x \in B \cap C$. Then $x \in B$ and $x \in C$. Since $x \in B$, it follows that $x \in A \cup B$. Since $x \in C$, it follows that $x \in A \cup C$. Thus $x \in (A \cup B) \cap (A \cup C)$.

($\supset$) Suppose $x \in (A \cup B) \cap (A \cup C)$. Then $x \in A \cup B$ and $x \in A \cup C$. We wish to show that $x \in A \cup (B \cap C)$, i.e., $x \in A$ or $x \in B \cap C$. Suppose $x \notin A$. It is enough to show that $x \in B \cap C$. Since $x \in A \cup B$ and $x \notin A$, it follows that $x \in B$. Likewise, since $x \in A \cup C$, $x \in C$. Thus $x \in B \cap C$. $\square$

In this example we have written down a lot of the details, but not every single one. For example, at the bottom of the proof, we write

> Since $x \in A \cup B$ and $x \notin A$, it follows that $x \in B$. Likewise, since $x \in A \cup C$, $x \in C$. Thus $x \in B \cap C$.

If we wanted to include every single detail, we would write

> Since $x \in A \cup B$, $x \in A$ or $x \in B$. Since $x \notin A$, it follows that $x \in B$. Since $x \in A \cup C$, $x \in A$ or $x \in C$. Since $x \notin A$, it follows that $x \in C$. Thus $x \in A$ and $x \in C$, so $x \in B \cap C$.

However, we prefer to be concise and omit obvious steps, provided that the reader can easily follow the argument. Usually a proof is centered around a few simple ideas, and excessive writing will tend to obscure them.

We would like to mention one more thing about the union and intersection operations. These are **binary** operations, which means that they can only operate on two sets at once. If we want to take the union of three sets A, B, and C, there are two different ways we might do this: either

$$A \cup (B \cup C)$$

or

$$(A \cup B) \cup C.$$

But the associative property says that these two expressions are equal. So when we write

$$A \cup B \cup C,$$

we mean either of the two expressions above. Also, the commutative property implies that we can change the order in which A, B, and C appear. Likewise for intersection.

Similarly, if n is any positive integer and $A_1, A_2, \ldots, A_n$ are sets, then there is no ambiguity in the expressions

$$A_1 \cup A_2 \cup \ldots \cup A_n$$

and

$$A_1 \cap A_2 \cap \ldots \cap A_n.$$

The union of $A_1, A_2, \ldots, A_n$ is the set of all things which are in at least one of these n sets; the intersection of $A_1, A_2, \ldots, A_n$ is the set of all things which are in all n sets.

A.3 Set difference

The **difference** between two sets A and B, denoted by $A - B$, is defined as follows:

$$A - B := \{x \mid x \in A \text{ and } x \notin B\}.$$

Figure **??** gives a Venn diagram illustrating this operation. For example, $\mathbb{Z} \setminus \mathbb{N}$ is the set of negative integers. Some literature uses the notation '$A \setminus B$' instead of $A - B$.

The following are some basic properties of the set difference operation which you should remember.

De Morgan's laws.

$$A - (B \cup C) = (A - B) \cap (A - C)$$

$$A - (B \cap C) = (A - B) \cup (A - C)$$

Other facts.

$$A - B \subset A \qquad\qquad B \cap (A - B) = \emptyset$$

$$\begin{aligned} A - B = \emptyset &\iff A \subset B \\ A - B = A &\iff A \cap B = \emptyset \end{aligned}$$

Example. Prove that $A-(B\cup C)=(A-B)\cap(A-C)$.

($\subset$) Suppose $x\in A-(B\cup C)$. Then $x\in A$, and $x\notin B\cup C$. Since it is not true that $x\in B$ or $x\in C$, we know that $x\notin B$ and $x\notin C$. Since $x\in A$ and $x\notin B$, we have $x\in(A-B)$. Likewise, $x\in(A-C)$. Thus $x\in(A-B)\cap(A-C)$.

($\supset$) Suppose $x\in(A-B)\cap(A-C)$. Then $x\in A$, $x\notin B$, and $x\notin C$. It is not true that $x\in B$ or $x\in C$, so $x\notin(B\cup C)$. Thus $x\in A-(B\cup C)$. $\square$

There are many more set-theoretic identities which we have not listed. However, instead of memorizing a huge list of identities, it is better to figure out and prove identities as they are needed. In mathematical writing, one usually omits proofs of simple set identities. (But don't do that for the exercises in this chapter.)

Exercises.

1. List separately the elements and the subsets of $\{\{1,\{2\}\},\{3\}\}$. (There are 2 elements and 4 subsets.)
2. Explain why if $A\subset B$ and $B\subset C$, then $A\subset C$.
3. If a set has exactly n elements, how many subsets does it have? Why?
4. We have repeatedly used the words, '*the* empty set'. Is this justified? If A and B are both sets that contain no elements, then is A necessarily equal to B?
5. Which of the following statements are true, and which are false? Why?
   (a) $\{\{\emptyset\}\}\cup\emptyset=\{\emptyset,\{\emptyset\}\}$
   (b) $\{\{\emptyset\}\}\cup\{\emptyset\}=\{\emptyset,\{\emptyset\}\}$
   (c) $\{\emptyset,\{\emptyset\}\}\cap\{\{\emptyset\},\{\{\emptyset\}\}\}=\{\emptyset\}$
   (d) $\{\emptyset,\{\emptyset\}\}\cap\{\{\emptyset\},\{\{\emptyset\}\}\}=\{\{\emptyset\}\}$
6. Prove the all the properties of union, intersection, and set difference that we stated without proof in the text.
7. Show that $A\cap(B-C)=(A\cap B)-(A\cap C)$. Is it always true that $A\cup(B-C)=(A\cup B)-(A\cup C)$?
8. Find some more set theoretic identities and prove them.