Lecture Notes

Math 100 — Winter 2024
Introduction to Proof

University of California, Santa Cruz

Deewang Bhamidipati

with support from
Sophie Aiken & David Rubinstein

(all errors introduced are my own)

Last Updated: Tuesday 5th March, 2024

Contents

1 Introduction **4**
- 1.1 Chessboard Problems . . . 4
- 1.2 Interlude: Naming Conventions . . . 7
- 1.3 The Pigeonhole Principle . . . 8

2 Direct Proofs **11**
- 2.1 Working from First Principles, i.e., Definitions . . . 11
- 2.2 Proofs by Cases . . . 13
- 2.3 Divisibility . . . 14
- 2.4 Greatest Common Divisor . . . 16
- 2.5 Modular Arithmetic . . . 18
- 2.6 Some Inequalities (skipped in class) . . . 21

3 Sets **23**
- 3.1 Set Theoretic Definitions . . . 23
- 3.2 Set Containment . . . 25
- 3.3 Set Equality . . . 27
- 3.4 Set Operations . . . 28

4 Induction **34**
- 4.1 A Chain Reaction . . . 34
- 4.2 Examples, examples, examples . . . 36
- 4.3 Strong Induction . . . 40
- 4.4 Non-examples . . . 44

5 Logic **46**
- 5.1 Statements . . . 46
- 5.2 Truth Tables . . . 48
- 5.3 Quantifiers and Negations . . . 51
- 5.4 Proving Quantified Statements . . . 54

6 The Contrapositive **56**
- 6.1 Finding the Contrapositive . . . 56
- 6.2 Proofs using Contrapositive . . . 57

7 Contradiction **61**
- 7.1 Contradiction & Examples . . . 61
- 7.2 Most Famous Proofs in History . . . 64

8 Functions **66**
- 8.1 Approaching Functions . . . 66
- 8.2 Injections, Surjections and Bijections . . . 69
- 8.3 The Composition . . . 74
- 8.4 Invertibility . . . 77

9 Relations **82**
9.1 Equivalence Relations 82

Lectures

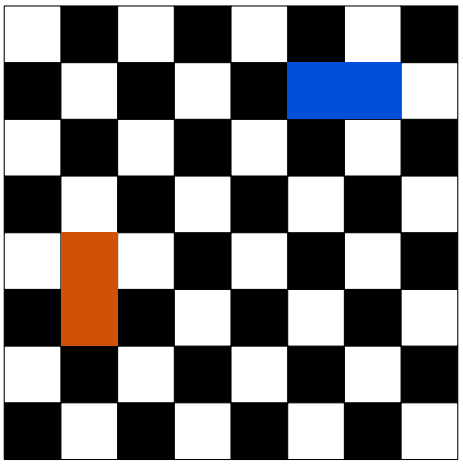
- Lecture 1 (01/08), page 3
- Lecture 2 (01/10), page 6
- Lecture 3 (01/12), page 10
- Lecture 4 (01/17), page 13
- Lecture 5 (01/19), page 16
- Lecture 6 (01/22), page 18
- Lecture 7 (01/24), page 22
- Lecture 8 (01/26), page 24
- Lecture 9 (01/29), page 28
- Lecture 10 (01/31), page 21
- Lecture 11 (02/02), page 34
- Lecture 12 (02/05), page 38
- Lecture 13 (02/07), page 42
- Lecture 14 (02/09), page 45
- Lecture 15 (02/12), page 47
- Lecture 16 (02/14), page 50
- Lecture 17 (02/16), page 53
- Lecture 18 (02/21), page 57
- Lecture 19 (02/23), page 61
- Lecture 20 (02/26), page 64
- Lecture 21 (02/28), page 67
- Lecture 22 (03/01), page 69
- Lecture 23 (03/04), page 72
- Lecture 24 (03/06), page 75

1. Introduction

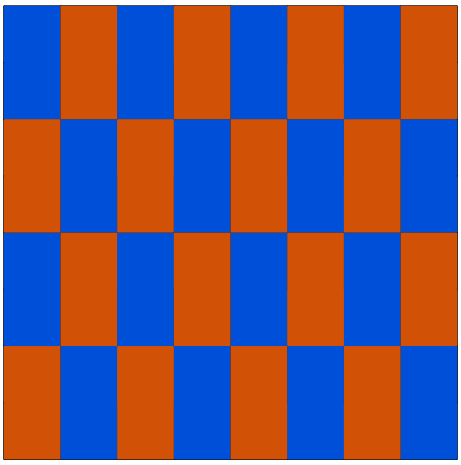
1.1. Chessboard Problems

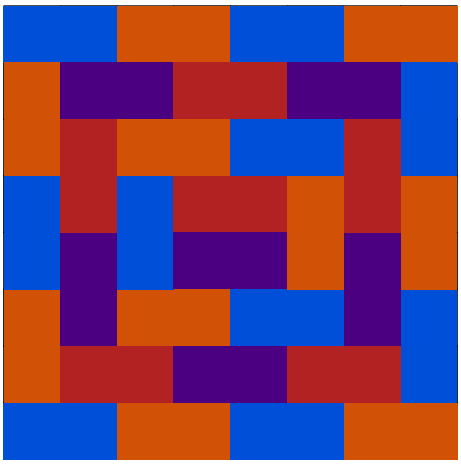
Lecture 1

Suppose one has a chessboard (8×8 square grid) and a bunch of dominoes (2×1 square blocks), so each domino can *perfectly* cover two squares on the chessboard.



Note that, with 32 dominoes we can cover the entire chessboard. There are many ways to achieve this. Here are two different ways we can go about covering the entire chessboard





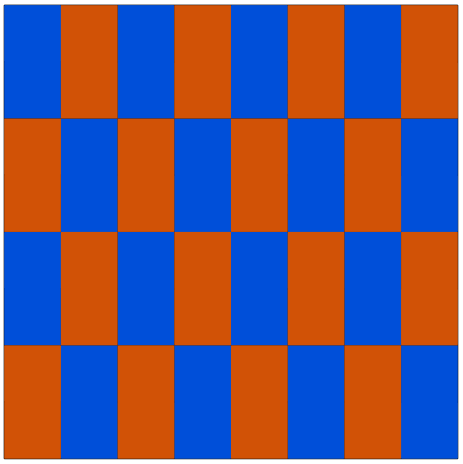
This motivates a definition.

Definition 1.1 (Perfect Cover)**.** A **perfect cover** of an $m \times n$ board with 2×1 dominoes is an arrangement using those dominoes on the chessboard with no squares left uncovered, no dominoes stacked and no dominoes going beyond the board.

Proposition 1.2. *There exists a perfect cover of an* 8×8 *board.*

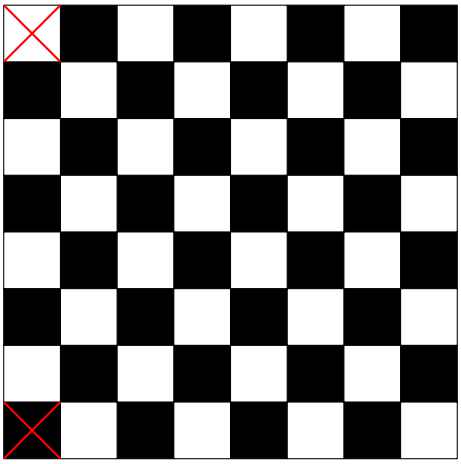
PROOF IDEA. There exists = provide at least one example.

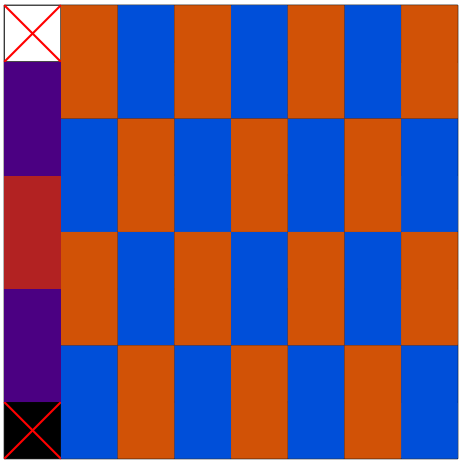
Proof. Observe that the following is a perfect cover.



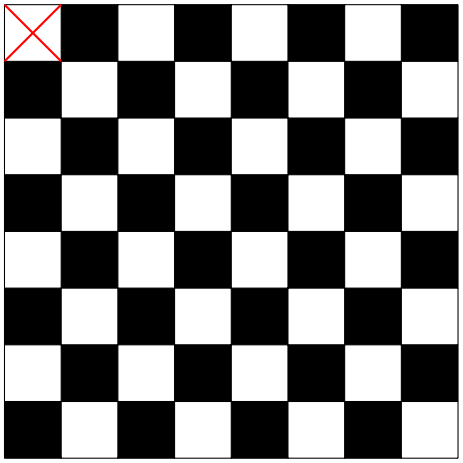
We have shown by example that a perfect cover exists, thus completing the proof. □

Suppose we cross out the bottom-left and top-left squares. We can still cover the 62 remaining squares. For example, one observes





What if we instead only cross out the top-left square?

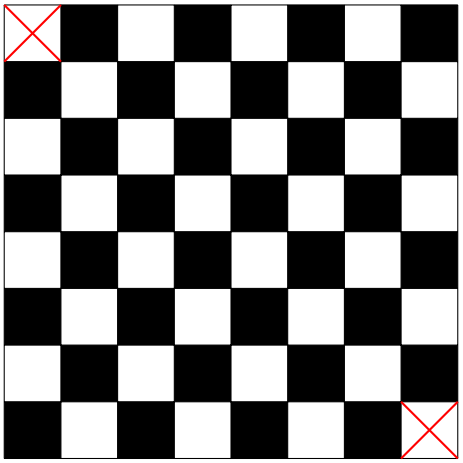


Proposition 1.3. *If one crosses out the top-left square of an* 8×8 *chessboard, then the remaining squares cannot be perfectly covered by* 2×1 *dominoes.*

PROOF IDEA. Dominoes cover even number of squares, while our chessboard has odd number of squares remaining!

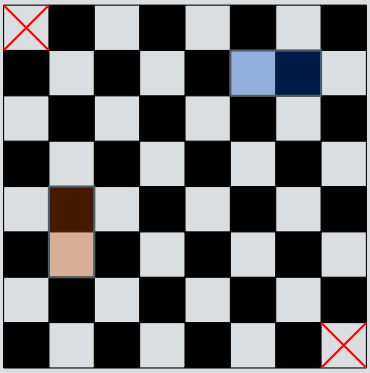
Proof. Since each domino covers 2 squares, and the dominoes are non-overlapping, if one places k *dominoes* on the board, they will cover $2k$ *squares*, which is always an *even number*. Therefore, a perfect cover can only cover an *even* number of squares. But we note that 63 is an *odd* number. Hence, the given board cannot be perfectly covered. □

Another scenario to consider is: what if we cross out the bottom-right and top-left squares?



Proposition 1.4. *If one crosses out the top-left and bottom-right squares of an* 8×8 *chessboard, then the remaining squares cannot be perfectly covered by* 2×1 *dominoes.*

PROOF IDEA. One domino covers exactly one dark and one light square.



Proof. The chessboard has 62 remaining squares, therefore we require

$$\frac{62}{2} = 31 \text{ dominoes}$$

to perfectly cover the board. Since each domino covers exactly one dark square and one light square, 31 dominoes placed non-overlappingly will cover 31 dark squares and 31 light squares.

But our given chessboard has 32 dark squares and 30 light squares. Therefore, it is impossible for 31 dominoes to cover these given 62 squares. □

1.2. Interlude: Naming Conventions

Lecture 2

We assign names to results to give them some contextual meaning and placement.

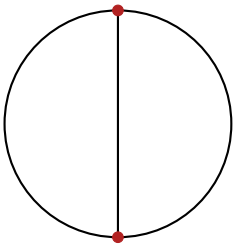
Convention 1.5.

- A **theorem** is an "important result" that has been proved.
- A **proposition** is a result that has been proved that is "less important" than a theorem.
- A **lemma** is typically a result that is proved before a proposition or a theorem, and is used to prove the proposition or theorem.
- A **corollary** is a result that is proved after a proposition or a theorem, and which quickly follows from the proposition or theorem. It is often a special case of the proposition or theorem.

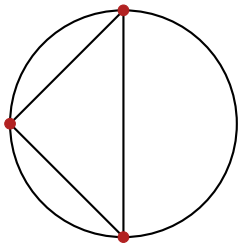
All of the above are results that have been proved.

Convention 1.6. A **conjecture** is a statement that we are hopeful is true but we have yet to prove. In particular, a conjecture could be true or false.

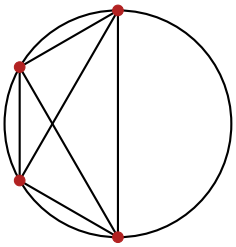
Example 1.7. Give a circle and $n > 1$ points placed randomly on its boundary. Let R_n denote the maximum number of regions created when we join all n points with a line segment.



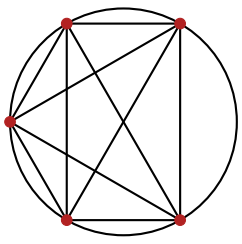
$R_2 = 2$



$R_3 = 4$



$R_4 = 8$

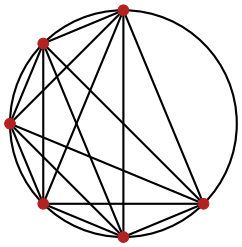


$R_5 = 16$

From these examples, we may conjecture

Conjecture 1.8. $R_n = 2^{n-1}$

But consider the case of $n = 6$



where we observe $R_6 = 31$, we conclude that our conjecture is *false*.

1.3. The Pigeonhole Principle

We wish to prove the following proposition.

Proposition 1.9. *Among any* 37 *people, at least* 4 *have the same birth-month.*

Remark 1.10. The mathematical idea that will help us prove this proposition is called the *Pigeonhole Principle*. Its name comes from a straightforward real-word observation: if there are 6 pigeons that live in 5 pigeonholes, then at least 1 pigeonhole has at least 2 pigeons living in it.

Likewise, if 11 or more pigeons that live in these 5 pigeonholes, then at least 1 pigeonhole has at least 3 pigeons living in it.

More generally, if $kn + 1$ or more pigeons that live in these n pigeonholes, then at least 1 pigeonhole has at least $k + 1$ pigeons living in it.

Wondrously, this principle more broadly beyond the case of pigeons.

Proof. We wish to prove our proposition using the Pigeonhole Principle; to apply the principle, we identify our pigeons and pigeonholes. We have that the

pigeons are the 37 people; and
pigeonholes are the 12 months

There is at least one month in which one of our 37 people have their birthday in.

It is not possible for each month to contain exactly 1 person's birthday, since that would account for only 12 of our 37 people, therefore at least one month contains at least 2 people's birthdays.

It is not possible for each month to contain exactly 2 people's birthday, since that would account for only 24 of our 37 people, therefore at least one month contains at least 3 people's birthdays.

It is not possible for each month to contain exactly 3 people's birthday, since that would account for only 36 of our 37 people, therefore at least one month contains at least 4 people's birthdays.

Thus, at least 4 people share the same birthmonth, amongst our group of 37 people. □

Principle 1.11 (Pigeonhole Principle)**.** *Assume n and k are positive integers. The* ***Pigeonhole Principle*** *states that*

(Simple form) *if $n+1$ objects are placed into n boxes, then at least 1 box has at least 2 objects in it.*

(General form) *if $kn+1$ objects are placed into n boxes, then at least 1 box has at least $k+1$ objects in it.*

Example 1.12. Given 5 playing cards, at least two cards have the same suit.

Proposition 1.13. *Given any 5 numbers from the set $\{1,2,3,4,5,6,7,8\}$, (at least) two of the chosen numbers will add up to 9.*

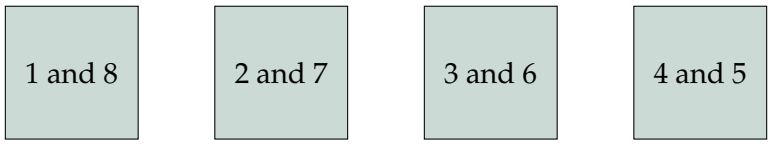
PROOF IDEA. There are four ways to obtain 9 as a sum of two numbers from the given set

$$1+8=8+1=9 \qquad 2+7=7+2=9 \qquad 3+6=6+3=9 \qquad 4+5=5+4=9$$

Proof. We wish to apply the Pigeonhole Principle; we identify our pigeons and pigeonholes. We have:

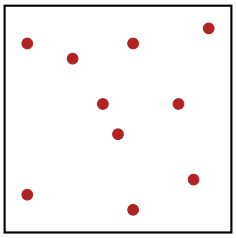
pigeons are the 5 numbers we chose from the set $\{1,2,3,4,5,6,7,8\}$; and

the pigeonholes are



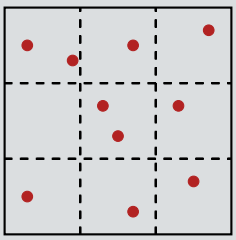
Therefore, by the Pigeonhole principle, at least one of these boxes has at two numbers in them. Necessarily, since these two numbers are distinct, they add up to 9. This proves our claim. □

Proposition 1.14. *Given a 3×3 box and any collection of 10 points in the box.*



At least two points have distance at most $\sqrt{2}$.

PROOF IDEA. Divide the 3×3 box into nine 1×1 boxes



Proof. We wish to apply the Pigeonhole Principle; we identify our pigeons and pigeonholes. We have that the

$$\text{pigeons are the 10 points; and}$$
$$\text{pigeonholes are the 9 boxes of size } 1 \times 1$$

Therefore, by the Pigeonhole principle, at least one of these 1×1 boxes has at two points in them.



The distance between these two points is necessarily less than the largest length they can have, which is the length of the diagonal of the 1×1 square. Therefore, the distance between these two points are at most $\sqrt{2}$, the length of the diagonal of the 1×1 square. □

2. Direct Proofs

Lecture 3

Suppose you overhear someone make the claim

every perfect number is even

and you may be forced to ask the question – what in the world is a *perfect number*? Decisions are important in mathematics, they are a synthesis of concrete observations, and give us precision. Mathematics is deep, and definitions often serve as geographical markers to help us precisely phrase the mathematics we wish to study and understand.

Deciding on a definition can be hard, and very often mathematicians have historically disagreed on definitions before coming to a general consensus (something that has happened for many definitions). To appreciate the difficulty, try coming up with a definition of a sandwich; you will quickly find a few counterexamples to your initial few attempts.

Therefore, if we wish to prove the above statement, it is important for us to know what the definition of a perfect number. In fact, we may even wish to ask for a precise definition of an *even number*.

We recall the following basic facts about the set of integers $\mathbb{Z}$

Fact 2.1. The sum of integers is an integer. The difference of integers is an integer. The product of integers is an integer. Finally, we have the principle of **parity** – every integer is either odd or even.

2.1. Working from First Principles, i.e., Definitions

Definition 2.2 (Odd & Even Integers)**.**

- An integer n is **even** if $n = 2k$ for *some integer* k.
- An integer n is **odd** if $n = 2k + 1$ for *some integer* k.

Example 2.3.

- 6 is even since $6 = 2 \cdot 3$, and 3 is an integer.
- 9 is odd since $9 = 2 \cdot 4 + 1$, and 4 is an integer.
- 0 is even since $0 = 2 \cdot 0$, and 0 is an integer.
- -15 is odd since $-15 = 2 \cdot (-8) + 1$, and -8 is an integer.

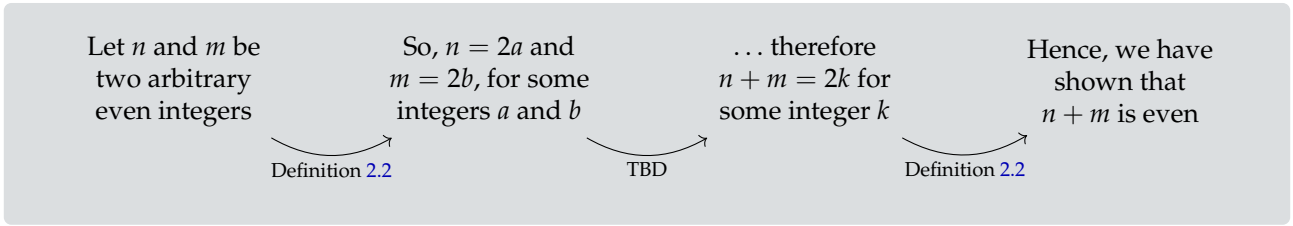
We will now prove a few results using these definitions.

Proposition 2.4. *The sum of two even integers is an even integer.*

PROOF IDEA. We will restate the statement a little bit: if two integers are even, then their sum is even. That is,

if n and m are even integers, then $n + m$ is an even integer.

Therefore the steps of our proof should be of the form



Proof. Let n and m be two arbitrary even integers. Therefore, by Definition 2.2, we must have $n = 2a$ and $m = 2b$ for some integers a and b. Hence,

$$n + m = 2a + 2b = 2(a + b)$$

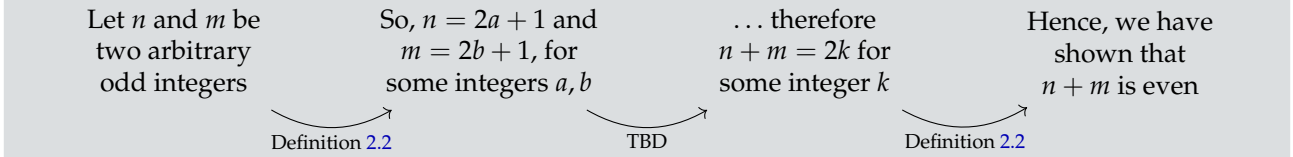
Since a and b are integers, so is $k = a + b$ (Fact 2.1), and thus $n + m = 2k$ is even, by Definition 2.2. □

Proposition 2.5. *The sum of two odd integers is an even integer.*

PROOF IDEA. As in Proposition 2.4, we wish to show that

if n and m are odd integers, then $n + m$ is an even integer.

Therefore the steps of our proof should be of the form



Proof. Let n and m be two arbitrary odd integers. Therefore, by Definition 2.2, we must have $n = 2a + 1$ and $m = 2b + 1$ for some integers a and b. Hence,

$$n + m = (2a + 1) + (2b + 1) = 2a + 2b + 2 = 2(a + b + 1)$$

Since a and b are integers, so is $a + b + 1$ (Fact 2.1), and thus $n + m$ is even, by Definition 2.2. □

Proposition 2.6. *If n is an odd integer, then n^2 is an odd integer.*

Proof. Assume n is an odd integer. Therefore, by Definition 2.2, we must have $n = 2a + 1$ for some integer a. Hence,

$$n^2 = (2a + 1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$$

Since a is an integer, so is $k = 2a^2 + 2a$ (Fact 2.1), and thus $n^2 = 2k + 1$ is odd, by Definition 2.2. □

Discussion 2.7 (if . . ., then . . . statements)**.** You may have noticed that the statements of the propositions, perhaps with a little amount of rewriting as done in the sketch, that we have discussed take on the following form

if *some statement is true*, then *some other statement is also true*

For example,

- If *you live in Santa Cruz*, then *you live in California*.
- If *m and n are even*, then $m + n$ *is even*.

Another way to write these statements is as follows:

some statement is true implies *some other statement is also true*

So, we may restate (one of) our statement(s) above as

m and n are even implies $m + n$ *is even*

Since so many of the statement we wish to prove are of this form, we have a special symbol for the word "implies", which is $\Rightarrow$, to use as a shorthand. In this shorthand, the above statement is

$$m \text{ and } n \text{ are even} \Rightarrow m + n \text{ is even}$$

Therefore, a general *if . . ., then . . .* statement is of the form

$$P \Rightarrow Q$$

where P and Q denote statements. We call P the *hypothesis*, and Q the *conclusion*.

⚠ **Warning.** The symbol $\Rightarrow$ is a mathematical shorthand for the word "implies" and therefore does not belong in a proof. It is a symbol we may readily use in our scratch work. While writing a proof, please use the word "implies" and avoid using the symbol $\Rightarrow$.

Discussion 2.8 (Direct Proofs)**.** The proofs we have seen in Propositions 2.4, 2.5 and 2.6 are examples of a *direct proof*. A **Direct Proof** is a way to prove a "$P \Rightarrow Q$" statement, by starting with the hypothesis P and working our way to the conclusion Q. The "working our way" may involve the use of definitions, previous results, algebra, logic and other techniques. Here is the general structure of a direct proof:

Proposition. $P \Rightarrow Q$

Proof. Assume P.

an explanation of what P means (apply definitions and/or other results)

⋮ apply algebra, logic and other techniques

Look, that is what Q means

Therefore Q. □

2.2. Proofs by Cases

Discussion 2.9. A related proof strategy is **Proof by Cases**. This is a "divide and conquer" strategy, where one breaks up their work into two or more cases that exhaust the hypothesis.

We will see an example that will illustrate this method of proof. Once we have broken our problem into cases, these cases still need to be proven, and one often proves these cases by using the strategy of a direct proof.

Proposition 2.10. *If n is an integer, then* $n^2 + n + 6$ *is even.*

PROOF IDEA. At this point, if we were asked to prove the statement *if n is an even integer, then n^2+n+6 is even* or the statement *if n is an odd integer, then n^2+n+6 is even*, then one can prove them directly the way we did in Propositions 2.4, 2.5 and 2.6.

Since we are being asked to prove this statement for *every integer n*, we may use Fact 2.1 to realise that an integer is either even or odd. This gives us our two cases: either n is even or n is odd. If we prove the proposition in these two cases, we will have proven the statement for all integers. That is what a proof by cases is all about.

Proof. Assume that n is an integer. Then n is either even or odd.

CASE 1. n is even

Assume n is even. Then $n = 2a$ for some integer a. Therefore,

$$\begin{aligned} n^2+n+6 &= (2a)^2+(2a)+6 \\ &= 4a^2+2a+6 \\ &= 2(2a^2+a+3) \end{aligned}$$

Since a is an integer, so is $k = 2a^2+a+3$ (Fact 2.1), and hence $n^2+n+6 = 2k$ is even, by Definition 2.2.

CASE 2. n is odd

Assume n is odd. Then $n = 2a+1$ for some integer a. Therefore,

$$\begin{aligned} n^2+n+6 &= (2a+1)^2+(2a+1)+6 \\ &= (4a^2+4a+1)+(2a+1)+6 \\ &= 4a^2+6a+8 \\ &= 2(2a^2+3a+4) \end{aligned}$$

Since a is an integer, so is $k = 2a^2+3a+4$ (Fact 2.1), and hence $n^2+n+6 = 2k$ is even, by Definition 2.2.

Thus, we have shown that n^2+n+6 is even whenever n is even or odd. Combined, this shows that n^2+n+6 is even for any integer n, as we wished to prove. □

2.3. Divisibility

Lecture 4 (see lecture recording to see a discussion that motivates the following definition)

Definition 2.11 (Divisibility)**.** A non-zero integer a is said to *divide* an integer b if

$$b = ak, \quad \text{for some integer } k.$$

When a divides b, we write $a \mid b$, and when a does not divide b we write $a \nmid b$.

Example 2.12.

- $2 \mid 22$ because $22 = 2 \cdot 11$ and 11 is an integer.
- $-5 \mid 30$ because $30 = (-5) \cdot (-6)$ and -6 is an integer.
- $12 \mid -48$ because $-48 = 12 \cdot (-4)$ and -4 is an integer.
- $-7 \mid 7$ because $7 = (-7) \cdot (-1)$ and -1 is an integer.
- $6 \nmid 9$ because $9 \neq 6k$ for any integer k (since we may write $9 = 6 \cdot (1.5)$, but 1.5 is not an integer).
- $a \mid 0$, for every non-zero integer a, because $0 = a \cdot 0$ and 0 is an integer.

Definition 2.13 (Divisor)**.** Given an integer n, we say an integer d is a **divisor** of n if $d \mid n$. Moreover, we call a divisor $d \neq \pm n$ a **proper divisor** of n.

Example 2.14.

- 2 and 11 are divisors of 22.
- -5 and 6 are divisors of 30.
- 12 and -4 are divisors of -48.
- -7 and -1 are divisors of 7.
- 6 is not a divisor of 9.
- every integer is a divisor of 0.

Definition 2.15 (Perfect Numbers)**.** A positive integer n is called a **perfect number** if the sum of all positive proper divisors of n equals n

Example 2.16.

- 6 is a perfect number, since its positive proper divisors are 1, 2 and 3, and

$$1 + 2 + 3 = 6.$$

- 28 is a perfect number, since its positive proper divisors are 1, 2, 4, 7 and 14, and

$$1 + 2 + 4 + 7 + 14 = 28.$$

The next two perfect numbers are 496 and 8128. You may see the sequence of known perfect numbers on The On-line Encyclopedia of Integer Sequences (OEIS) – A000396.

Some important conjectures regarding perfect numbers that have yet to be proven in complete generality are:

- Are there any odd perfect numbers?
- Are there infinitely many perfect numbers?

Proposition 2.17 (Transitivity of Divisibility)**.** *Let a, b and c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.*

Proof. Our proof will follow the structure presented in Discussion 6.4.

Assume that a, b and c are integers, such that $a \mid b$ and $b \mid c$. Then, by Definition 2.11, we have $b = as$ and $c = bt$, for some integers s and t. Therefore,

$$c = bt = (as)t = a(st)$$

Since s and t are integers, so is $k = st$ (Fact 2.1), and hence $c = ak$. Thus $a \mid c$, by Definition 2.11. □

Discussion 2.18 (The Division Algorithm)**.** It is often the case that two integers do not divide each other. For examples, $6 \nmid 9$ and $3 \nmid 7$. One way we see this is by seeing that if we do try to divide, say 7 by 3, we would be left with a remainder, i.e.

$$7 = 3 \cdot 2 + 1$$

Here 2 is called the *quotient* and 1 is called the *remainder*. This fact, that we can relate a pair of numbers in such a way, is called the **division algorithm**.

Theorem 2.19 (The Division Algorithm)**.** *For all integers a and m with $m > 0$, there exist* unique *integers q and r such that*

$$a = mq + r, \quad \text{where } 0 \leqslant r < m$$

Remark 2.20. Observe that in Theorem 2.19, if $m = 2$, then we have two possibilities for a and they are: $a = 2q + 0$ or $a = 2q + 1$; these are the definitions of even and odd numbers. Moreover, if $r = 0$, then this gives us $a = mq$, which is our definition of divisibility, in this case $m \mid a$.

Here are a few more examples of the division algorithm in action

Example 2.21.

- If $a = 18$ and $m = 7$, then $18 = 7 \cdot 2 + 4$. Note that $0 \leqslant 4 < 7$.
- If $a = 13$ and $m = 3$, then $13 = 3 \cdot 4 + 1$. Note that $0 \leqslant 1 < 3$.
- If $a = 35$ and $m = 5$, then $35 = 5 \cdot 7 + 0$. Note that $0 \leqslant 0 < 5$.
- If $a = -18$ and $m = 7$, then $-18 = 7 \cdot (-3) + 3$. Note that $0 \leqslant 3 < 7$.
- If $a = 3$ and $m = 13$, then $3 = 13 \cdot 0 + 3$. Note that $0 \leqslant 3 < 13$.

2.4. Greatest Common Divisor

Definition 2.22 (Greatest Common Divisor)**.** Let a and b be integers. If c is any integer such that $c \mid a$ and $c \mid b$, then c is said to be a *common divisor*.

The **greatest common divisor** (gcd) of a and b is the largest common divisor d of a and b. That is,

(D1) d is a common divisor, i.e., $d \mid a$ and $d \mid b$; and

(D2) d is the largest common divisor, i.e., if c is any other common divisor of a and b, then $c \leqslant d$.

The greatest common divisor (gcd) of a and b is denoted as $\gcd(a, b)$.

Suppose a and b are non-zero. Note that since $1 \mid a$ and $1 \mid b$, we have that 1 is a common divisor of a and b, and therefore $1 \leqslant \gcd(a, b)$, the *largest* common divisor. Moreover, since the gcd divides a and b, we must have $\gcd(a, b) \leqslant |a|$ and $\gcd(a, b) \leqslant |b|$. Hence, we have that

$$1 \leqslant \gcd(a, b) \leqslant \min\{|a|, |b|\}$$

Example 2.23. Here are some examples of gcds.

- $\gcd(6, 8) = 2$
- $\gcd(6, -8) = 2$
- $\gcd(-5, -20) = 5$
- $\gcd(12, 8) = 4$
- $\gcd(7, 15) = 1$
- $\gcd(9, 9) = 9$

Lecture 5

Theorem 2.24 (Bézout's Identity)**.** *If a and b are positive integers, then there exist integers k and ℓ such that*

$$\gcd(a, b) = ak + b\ell$$

PROOF IDEA. To make sure we understand the statement, let's work out on example. Let's consider $a = 15$ and $b = 21$, making $\gcd(15, 21) = 3$. The claim is that we can find integers k and ℓ such that

$$3 = \gcd(15, 21) = 15k + 21\ell$$

Testing a few numbers gives us

$$3 = 15(3) + 21(-2)$$

or maybe one also found

$$3 = 15(-4) + 21(3)$$

Indeed, there are infinitely such k and ℓ. Nevertheless, the theorem states that one such pair exists.

The general structure of our proof is

1. Assume a and b are positive integers; these are fixed quantities, and therefore so is $\gcd(a, b)$. Despite being fixed quantities, we don't know which numbers they are exactly as we wish to prove this in complete generality. Our choices for k and ℓ are not free, we have one constraint: $ak + b\ell = \gcd(a, b)$.
2. Turns out, there's a clever way to pick k and ℓ. Once we pick them, we still need to show that they work. That is, once we choose them, we will call $d = ak + b\ell$. Our task will be to show $d = \gcd(a, b)$.
3. To show $d = \gcd(a, b)$, we will show that d is common divisor, and greater than any other common divisor of a and b.

The most difficult step will be Step 3. Let's get into the proof!

Proof. Assume that a and b are fixed positive integers. Notice that, for any choice of a pair (x, y) of integers, the expression $ax + by$ can take different values, including positive ($x = y = 1$), negative

($x = y = -1$) and even zero ($x = y = 0$). Let d be the smallest positive value that $ax + by$ can equal. Let k and ℓ be the integers that give us d. That is, for these integers k and ℓ we obtain

$$d = ak + b\ell \tag{☂}$$

We will now prove that this d is $\gcd(a, b)$.

(D1) *d is a common divisor of a and b*

We wish to prove that $d \mid a$ and $d \mid b$. Let us try and prove $d \mid a$. By the division algorithm (Theorem 2.19), there exist integers q and r such that

$$a = dq + r$$

where $0 \leqslant r < d$. Rewriting the above expression, we get

$$\begin{aligned} r &= a - dq \\ &= a - (ak + b\ell)q && \text{using (☂)} \\ &= a - ak - bq\ell \\ &= a(1 - k) + b(-q\ell) \end{aligned}$$

Hence $0 \leqslant r < d$ is an integer of the form $ax + by$ for $x = 1 - k$ and $y = -q\ell$. But we chose d to be the smallest such positive integer; thus necessarily we must have that $r = 0$. Therefore $a = dq$ and hence $d \mid a$.

One can similarly show that $d \mid b$. Hence, d is a common divisor of a and b.

(D2) *d is the largest common divisor of a and b*

Suppose that c is some other common divisor of a and b. We wish to prove that $c \leqslant d$. Since $c \mid a$ and $c \mid b$, we have (Definition 2.11)

$$a = cm \quad \text{and} \quad b = cn$$

for some integers m and n. Applying this to (☂) above, we obtain

$$\begin{aligned} d &= ak + b\ell \\ &= cmk + cn\ell \\ &= c(mk + n\ell) \end{aligned}$$

Since m, n, k and ℓ are integers, so is $mk + n\ell$ (Fact 2.1) and therefore $c \mid d$. Which, in particular, tells us that $c \leqslant d$, since $d > 0$.

Thus, $\gcd(a, b) = d = ak + b\ell$ which completes the proof. □

2.5. Modular Arithmetic

The division algorithm tells us that if an integer a is divided by an integer $m > 0$, then there are unique integers q and r such that

$$a = mq + r, \quad \text{where } 0 \leqslant r < m$$

Turns out, the relationship between a and its remainder, when divided b, r is surprisingly important.

Definition 2.25 (Modular Congruence)**.** For integers a, r and m, we say that ***a* is congruent to *r* modulo *m***, and we write $a \equiv r \bmod m$, if $m \mid (a - r)$.

Example 2.26. Let us revisit Example 2.21, we observe that

- $18 \equiv 4 \bmod 7$
- $35 \equiv 0 \bmod 5$
- $3 \equiv 3 \bmod 13$
- $13 \equiv 1 \bmod 3$
- $-18 \equiv 3 \bmod 7$
- $-3 \equiv 2 \bmod 2$

But it is important to note that Definition 2.25 is not referencing the remainders at all. Therefore, one may also observe the following

- $18 \equiv 11 \bmod 7$
- $35 \equiv 30 \bmod 5$
- $3 \equiv 16 \bmod 13$
- $1 \equiv 13 \bmod 3$
- $-18 \equiv -4 \bmod 7$
- $-3 \equiv -3 \bmod 2$

Lecture 6 (box metaphor and clock metaphor in class)

Proposition 2.27 (Modular Arithmetic)**.** *Assume that a, b, c, d and m are integers such that $a \equiv b \bmod m$ and $c \equiv d \bmod m$. Then,*

(i) $a + c \equiv b + d \bmod m$

(ii) $a - c \equiv b - d \bmod m$

(iii) $a \cdot c \equiv b \cdot d \bmod m$

Proof. We prove (i), and leave (ii) and (iii) as an exercise.

Assume a, b, c, d and m are integers such that $a \equiv b \bmod m$ and $c \equiv d \bmod m$. By Definition 2.25, we have $m \mid (a - b)$ and $m \mid (c - d)$. Therefore,

$$a - b = mk \quad \text{and} \quad c - d = m\ell$$

for some integers k and ℓ. Hence, we observe that

$$\begin{aligned}(a + c) - (b + d) &= (a - b) + (c - d) \\ &= mk + m\ell \\ &= m(k + \ell)\end{aligned}$$

Since k and ℓ are integers, so is $k + \ell$, and thus $m \mid ((a + c) - (b + d))$, by Definition 2.11. Therefore, $a + c \equiv b + d \bmod m$, as we wished to show. □

Remark 2.28. Proposition 2.27 tells us that modular arithmetic has nice properties for addition, subtraction and multiplication. What about division? Well, not always! Try an example: find integers a, b, k and m such that $ak \equiv bk \bmod m$ but $a \not\equiv b \bmod m$.

Now, try and find an example where $ak \equiv bk \bmod m$ and $a \equiv b \bmod m$.

In these two examples, describe the relation between k and m.

Definition 2.29 (Prime Numbers)**.** An integer $p \geqslant 2$ is **prime** if its only positive divisors are 1 and p.

An integer $n \geqslant 2$ is **composite** if it is *not prime*. That is, n is composite if it can be written as $n = st$, where s and t are integers and $1 < s,\ t < n$.

Lemma 2.30. *Let a, b and c are integers, and let p be a prime.*

(i) If $p \nmid a$, then $\gcd(a, p) = 1$.

(ii) If $a \mid bc$, and $\gcd(a, b) = 1$, then $a \mid c$.

(iii) If $p \mid bc$, then $p \mid b$ or $p \mid c$.

Proof.

(i) Assume a is an integer and p is a prime number such that $p \nmid a$. We wish to show that $\gcd(a, p) = 1$; let $d = \gcd(a, p)$. Observe that $p \mid p$ but $p \nmid a$, by assumption, and hence p is *not* a common divisor of a and p. Thus, $d \neq p$. Since p is prime, its positive divisors are 1 and p, and as we have already observed that $d \neq p$, we must have $d = 1$. Therefore $\gcd(a, p) = 1$.

(ii) Assume a, b and c are integers such that $a \mid bc$ and $\gcd(a, b) = 1$. We wish to show that $a \mid c$. Since $\gcd(a, b) = 1$, by Bézout's Identity (Theorem 2.24), there exist integers k and ℓ such that

$$ak + b\ell = \gcd(a, b) = 1$$

Multiplying both sides by c, we obtain

$$c = ack + bc\ell \qquad (\bigstar)$$

Furthermore, since we have also assumed $a \mid bc$, we have $bc = am$ for some integer m. Substituting in ($\bigstar$) we obtain

$$\begin{aligned} c &= ack + bc\ell \\ &= ack + am\ell \\ &= a(ck + m\ell) \end{aligned}$$

Since c, k, ℓ and m are integers, so is $ck + m\ell$. Therefore $a \mid c$, by Definition 2.11, as we wished to show.

(iii) Assume b, c are integers, and p is a prime number such that $p \mid bc$. We wish to show $p \mid b$ or $p \mid c$. We will provide a proof by cases, where our two cases are: $p \mid b$ or $p \nmid b$.

CASE 1. $p \mid b$

Since we wished to prove $p \mid b$ or $p \mid c$, we are immediately done. Since what we wish to show is already our assumption, and therefore no more work is needed!

CASE 2. $p \nmid b$

Since $p \nmid b$, by (i), we conclude that $\gcd(p, b) = 1$. Our assumption was $p \mid bc$, we may now apply (ii) to conclude $p \mid c$, as we wished to show.

In either case, we have concluded that $p \mid b$ or $p \mid c$, which is what we wished to show. □

Proposition 2.31 (Modular Cancellation Law)**.** *Assume that a, b, m, and k are integers, with $k \neq 0$. If $ak \equiv bk \bmod m$ and $\gcd(k, m) = 1$, then $a \equiv b \bmod m$.*

Proof. Assume that a, b, m, and k are integers, with $k \neq 0$, such that $ak \equiv bk \bmod m$. We wish to prove that $a \equiv b \bmod m$. By assumption, we have $m \mid (ak - bk)$. We make two observations: $\gcd(m, k) = \gcd(k, m) = 1$ and $ak - bk = k(a - b)$. Therefore, we have

$$m \mid (k(a - b))$$

Applying Lemma 2.30 (ii), we conclude $m \mid (a - b)$. Thus, $a \equiv b \bmod m$, as we wished to show. □

Theorem 2.32 (Fermat's Little Theorem)**.** *If a is an integer and p is a prime such that $p \nmid a$, then*

$$a^{p-1} \equiv 1 \bmod p.$$

2.6. Some Inequalities (skipped in class)

We end this chapter with an example of direct proofs where we branch out of number theory, and the middle computational step of a direct proof is of a different nature.

Proposition 2.33. *Assume that x and y are positive real numbers. If $x \geqslant y$, then $\sqrt{x} \geqslant \sqrt{y}$.*

PROOF IDEA. Before we discuss the mathematical ideas we may need to prove this proposition, let us recall the structure of a direct proof (Discussion 6.4).

- STEP 1. *State your assumptions.* Assume $x \geqslant y$.
- STEP 2. *An explanation of what the assumption means.* This is equivalent to $x - y \geqslant 0$.
- STEP 3. *Computational step: applying algebra, logic, techniques etc.* $(\cdots)$
- STEP 4. *Look, this is what the conclusion means.* Which implies $\sqrt{x} - \sqrt{y} \geqslant 0$.
- STEP 5. *Conclude.* Thus $\sqrt{x} \geqslant \sqrt{y}$.

Let us now focus on what our idea for Step 3 should be. We wish to go from $x - y \geqslant 0$ to the inequality $\sqrt{x} - \sqrt{y}$, so we wish to determine how we can relate $x - y$ to $\sqrt{x} - \sqrt{y}$. What will come handy here is the *difference of squares* identity: $a^2 - b^2 = (a - b)(a + b)$.

Proof. Assume that x and y are positive real numbers such that $x \geqslant y$. Therefore, $x - y \geqslant 0$.

We note that $x = (\sqrt{x})^2$ and $y = (\sqrt{y})^2$, and hence using the difference of squares identity, the left-hand side of the inequality above is of the form

$$x - y = (\sqrt{x})^2 - (\sqrt{y})^2 = (\sqrt{x} - \sqrt{y})(\sqrt{x} + \sqrt{y})$$

We may use this to rewrite our inequality as

$$(\sqrt{x} - \sqrt{y})(\sqrt{x} + \sqrt{y}) \geqslant 0$$

Since x and y are positive, so is $\sqrt{x}+\sqrt{y}$, and hence dividing by it in an inequality will not change the direction of the inequality. Thus, dividing by $\sqrt{x}+\sqrt{y}$ on both sides of the inequality above, we obtain

$$\sqrt{x}-\sqrt{y} \geqslant 0$$

Therefore, we get $\sqrt{x} \geqslant \sqrt{y}$, as we wished to show. □

We use the above proposition, to prove an important inequality which might be a bit less intuitive.

Theorem 2.34 (AM-GM Inequality)**.** *If x and y are positive real numbers, then*

$$\frac{x+y}{2} \geqslant \sqrt{xy}$$

SCRATCH WORK. Since we don't have a ton of assumptions, let us rely on the conclusion to synthesise a problem-solving strategy. It may seem strange, but we might be able to "reverse engineer" a problem-solving strategy. Let us start with

$$\frac{x+y}{2} \geqslant \sqrt{xy}$$

Let us multiply both sides by 2 (denominators are annoying)

$$x+y \geqslant 2\sqrt{xy}$$

Let us square both sides (since square roots are annoying)

$$x^2+2xy+y^2 \geqslant 4xy$$

Let us isolate the inequality of the left-hand side, by subtracting by $4xy$ on both sides

$$x^2-2xy+y^2 \geqslant 0$$

What do we notice the left-hand side to be?

How does this help with our proof? The wonder of this scratch work is that the steps we took are reversible (our Proposition 2.33) comes in handy!

Proof. Assume x and y are positive real numbers, and therefore so are $x+y$ and xy. Observe that we always have $(x-y)^2 \geqslant 0$, hence

$$\begin{aligned}
x^2-2xy+y^2 &\geqslant 0 && \\
x^2+2xy+y^2 &\geqslant 4xy && \text{adding } 4xy \text{ on both sides} \\
(x+y)^2 &\geqslant 4xy && \\
x+y &\geqslant 2\sqrt{xy} && \text{using Proposition 2.33, since } x+y \text{ and } xy \text{ are positive} \\
\frac{x+y}{2} &\geqslant \sqrt{xy} && \text{dividing by 2 on both sides}
\end{aligned}$$

which is what we wished to show. □

3. Sets

3.1. Set Theoretic Definitions

Lecture 7

Definition 3.1 (Sets)**.** A **set** is an *unordered* collection of distinct objects, which are called **elements**.

We will denote sets by upper-case letters $A, B, C, \ldots, X, Y, Z$, while elements will be denoted by lower-case letters $a, b, c, \ldots, x, y, z$.

We use $\in$ to denote membership of, or belongingness to, a set

$$x \in S : \text{read } \text{“}x \text{ in } S\text{”, i.e., } x \text{ is an element of a set } S$$
$$x \notin S : \text{read } \text{“}x \text{ not in } S\text{”, i.e., } x \textit{ is not } \text{an element of a set } S$$

When reasonable, sets are often written by listing all their elements and enclosing them within { }. For example, $\{2, \pi, 1/3\}$. We record some important sets and their notations.

Definition 3.2.

- The **set of integers**, denoted $\mathbb{Z}$, is the set $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- The **set of positive integers** $\{1, 2, 3, \ldots\}$ will be denoted as $\mathbb{Z}_{>0}$.
  Some authors refer to this set as $\mathbb{N}$.
- The **set of non-negative integers** $\{0, 1, 2, 3, \ldots\}$ will be denoted as $\mathbb{Z}_{\geqslant 0}$.
  Some authors refer to this set as $\mathbb{N}_0$.
- The set without any elements, denoted $\varnothing$ or $\{\ \}$, is called the **empty set**.

(box metaphor in class)

Discussion 3.3 (Set-Builder Notation)**.** All of our examples, thus far, have been sets written like $\{\ldots\}$, where enclosed within the braces are a list of the elements. Sometimes, though, they are defined by a rule; this is called *set-builder notation*. This notation looks like

$$\{\text{typical element } : \text{ conditions used to generate the elements}\}$$

or

$$\{\text{element} \in S \ : \ \text{conditions used to generate the elements}\}$$

where S is some larger set in which the conditions are restricting.

Some examples of the first form are:

- $T = \{n^2 \ : \ n \in \mathbb{Z}_{>0}\} = \{1, 4, 9, 16, 25, \ldots\}$
- $A = \{|n| \ : \ n \in \mathbb{Z}\} = \{0, 1, 2, 3, 4, \ldots\}$

The first example, of the set T, uses the condition $n \in \mathbb{Z}_{>0}$ which means that you should plug in positive integers $n = 1, 2, 3, 4, 5, \ldots$ into n^2 to obtain the elements of the set. Moreover, if we are to consider an element $x \in T$, then the definition says that $x = n^2$ for some $n \in \mathbb{Z}_{>0}$.

Some examples of the second form are:

- $E = \{n \in \mathbb{Z} \ : \ n \text{ is even}\} = \{\ldots, -6, -4, 2, 0, 2, 4, 6, \ldots\}$
- $H = \{n \in \mathbb{Z}_{>0} \ : \ 6 \mid n\} = \{6, 12, 18, 24, 30, \ldots\}$

Remark 3.4. Be careful about using ..., this is not rigorous and is an informal way of saying "continue the pattern you see forever". Therefore, you should use them only when the pattern is indeed clear. For example, if one writes $1, 2, \ldots$, it is not at all clear what the ... reflect. Is this the sequence of all positive integers: $1, 2, 3, 4, 5, \ldots$? Is this this the sequence of powers of 2: $1, 2, 4, 8, 16, \ldots$? Is this is the sequence of factorial values: $1, 2, 6, 24, 120, \ldots$?

Thus, make sure the pattern you wish the reader to understand is very clear before adding the ...

Definition 3.5 (Rational Numbers)**.** The set

$$\mathbb{Q} = \left\{ \frac{a}{b} \ : \ a, b \in \mathbb{Z},\ b \neq 0 \right\}$$

is called the **set of rational numbers**.

One reads this notation as

$\mathbb{Q}$	$=$	$\{$	$\frac{a}{b}$	$:$	$a, b \in \mathbb{Z}$	$,$	$b \neq 0$
The rational numbers	are defined to be	the set of all	fractions of the form a/b	such that	a and b are integers	and	b is non-zero

Example 3.6. The set of real numbers, denoted $\mathbb{R}$, is much harder to define, so in this class we will rely on our intuition – real numbers are those numbers that can be written down with a decimal point. This includes integers like -4, fractions like $1/3 = 0.666\ldots$ and $1/2 = 0.5$, and numbers like $3.14159\ldots$.

Let us use $\mathbb{R}$ and set-builder notation to generate other familiar sets. The set of 2×2 real matrices can be written as

$$\mathrm{M}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ : \ a, b, c, d \in \mathbb{R} \right\}$$

The real plane represents the set of *ordered pairs* of real numbers. This set can be written as

$$\mathbb{R}^2 = \{(x, y) \ : \ x, y \in \mathbb{R}\}$$

The unit circle (the circle of radius 1 centered at the origin) can be defined as

$$S^1 = \{(x, y) \in \mathbb{R}^2 \ : \ x^2 + y^2 = 1\}$$

The closed interval $[a, b]$ for real numbers a and b can be defined as

$$[a, b] = \{x \in \mathbb{R} \ : \ a \leqslant x \leqslant b\}$$

One denotes an open interval as (a, b), which looks similar to an ordered pair, but context clues can help you determine which notion we are referring to with this notation

$$(a, b) = \{x \in \mathbb{R} \ : \ a < x < b\}$$

3.2. Set Containment

Definition 3.7 (Subsets)**.** Suppose A and B are sets. If every element of A is *also* an element of B, then A is a **subset** of B, and this is denoted $A \subseteq B$. That is, A is the set of *some* elements in B.

If A is *not a subset* of B, we write $A \not\subseteq B$, and this occurs if there is an element of A which is not in B.

It is also clear that if we have sets A, B and C with $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Lecture 8

Example 3.8.

- $\{1,3,5\} \subseteq \{1,2,3,5,7\}$, because 1, , 3 and 5 are all in the latter set $\{1,2,3,5,7\}$.
- $\mathbb{Z}_{>0} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$
- $\{a,b,c\} \not\subseteq \{a,b,e,f,g\}$, because $c \notin \{a,b,e,f,g\}$.
- Given any set S, it is always true that $S \subseteq S$ and $\varnothing \subseteq S$.

Definition 3.9 (Proper Subsets)**.** Suppose A and B are sets. We say A is a **proper subset** of B if $A \subseteq B$ and $A \neq B$. We denote this as $A \subset B$.

For example, $\mathbb{Z}_{>0} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Discussion 3.10 (Proving Set Containment)**.** Definition 3.7 tells us that in order to prove that $A \subseteq B$, what we have to prove is the statement

$$\textit{if } x \in A, \textit{ then } x \in B$$

Hence, for a (direct) proof that a set A is a subset of a set B, the outline will be:

Proposition. $A \subseteq B$

Proof. Assume $x \in A$.

an explanation of what $x \in A$ means

$\vdots$ apply algebra, logic and other techniques

Look, that is what $x \in B$ means

Therefore $x \in B$.

Since $x \in A$ implies $x \in B$, we have shown that $A \subseteq B$. □

Proposition 3.11. *It is the case that* $\{n \in \mathbb{Z} \,:\, 12 \mid n\} \subseteq \{n \in \mathbb{Z} \,:\, 3 \mid n\}$.

PROOF IDEA. To follow the outline of a set containment proof, we have

Proof. Assume $x \in \{n \in \mathbb{Z} \,:\, 12 \mid n\}$.

Therefore $x \in \mathbb{Z}$ and $12 \mid x$, and hence $x = 12k$ for some integer k, by Definition 2.11.

$\vdots$ apply algebra, logic and other techniques

Therefore, $x = 3\ell$ for some $\ell \in \mathbb{Z}$. Hence $3 \mid x$, by Definition 2.11.

Thus $x \in \{n \in \mathbb{Z} : 3 \mid n\}$.

Since $x \in \{n \in \mathbb{Z} : 12 \mid n\}$ implies $x \in \{n \in \mathbb{Z} : 3 \mid n\}$, we have shown that

$$\{n \in \mathbb{Z} : 12 \mid n\} \subseteq \{n \in \mathbb{Z} : 3 \mid n\}.$$

Proof. Assume $x \in \{n \in \mathbb{Z} : 12 \mid n\}$. Therefore $x \in \mathbb{Z}$ and $12 \mid x$, and hence $x = 12k$ for some integer k, by Definition 2.11. Thus,

$$x = 12k = 3(4k)$$

Since $k \in \mathbb{Z}$, it is also true that $\ell = 3k \in \mathbb{Z}$, and therefore $x = 3\ell$ allows us to conclude $3 \mid x$, by Definition 2.11. Hence $x \in \{n \in \mathbb{Z} : 3 \mid n\}$.

Since $x \in \{n \in \mathbb{Z} : 12 \mid n\}$ implies $x \in \{n \in \mathbb{Z} : 3 \mid n\}$, we have shown the set containment we wished to show: $\{n \in \mathbb{Z} : 12 \mid n\} \subseteq \{n \in \mathbb{Z} : 3 \mid n\}$. □

Remark 3.12. We have seen in Discussion 3.10 and Proposition 3.13 that to prove $A \subseteq B$, we picked an *arbitrary* element x of A and then showed that $x \in B$. It is important that this was an arbitrary element and not a specific element of A, e.g., 24. Moreover, the only thing we are allowed to assume of x is that it is an element of A, therefore the only properties it has are the ones it obtains by being an element of A.

The reason this is important is because anything we prove about our arbitrary element of A will then apply to *every* element of A.

The next example may look a bit different, but the same general principles apply.

Proposition 3.13. *Let* $A = \{-1, 3\}$ *and* $B = \{x \in \mathbb{R} : x^3 - 3x^2 - x + 3 = 0\}$. *Then* $A \subseteq B$.

PROOF IDEA. Recall that we wish to prove that if $x \in A$, then $x \in B$. The main trick here is to realise that $x \in A$ can only mean one of two things: either $x = -1$ or $x = 3$. Since there are two distinct options, this suggests that we may use a proof by cases strategy.

How do we conclude that our choices of x are in B? We must show that such an x satisfies the equation $x^3 - 3x^2 - x + 3 = 0$. If it does, then we must have $x \in B$, since that is the defining property of elements of B.

Proof. Assume $x \in A = \{-1, 3\}$. Then either $x = -1$ or $x = 3$.

CASE 1. $x = -1$. Observe that x is a real number, and

$$(-1)^3 - 3(-1)^2 - (-1) + 3 = -1 - 3 + 1 + 3 = 0$$

Therefore, by definition, this implies $x \in B$.

CASE 2. $x = 3$. Observe that x is a real number, and

$$3^3 - 3(3)^2 - (3) + 3 = 27 - 27 - 3 + 3 = 0$$

Therefore, by definition, this implies $x \in B$.

Since $x \in A$ implies $x \in B$, we have shown that $A \subseteq B$. □

3.3. Set Equality

Remark 3.14. What does it mean to say two sets are equal, which makes sense to denote $A = B$? Equality of sets should mean that the two sets have *exactly* the same elements. Said differently, it should mean the following two things:

- Every element of A is also an element of B (i.e., $A \subseteq B$); and
- Every element of B is also an element of A (i.e., $B \subseteq A$); and

This motivates the definition of two sets being equal.

Definition 3.15 (Set Equality)**.** Given two sets A and B, we say A and B are **equal**, denoted $A = B$, if $A \subseteq B$ and $B \subseteq A$.

Discussion 3.16 (Proving Set Equality)**.** The outline of a sets equality proof is as follows:

Proposition. $A \subseteq B$

Proof. Assume $x \in A$.

an explanation of what $x \in A$ means

⋮ apply algebra, logic and other techniques

Look, that is what $x \in B$ means

Therefore $x \in B$.

Since $x \in A$ implies $x \in B$, we have shown that $A \subseteq B$.

Next, assume $x \in B$.

an explanation of what $x \in B$ means

⋮ apply algebra, logic and other techniques

Look, that is what $x \in A$ means

Therefore $x \in A$.

Since $x \in B$ implies $x \in A$, we have shown that $B \subseteq A$.

We have shown that $A \subseteq B$ and $B \subseteq A$. Therefore $A = B$. □

Remark 3.17. Observe that the definition of set equality is not unlike a strategy to show $x = y$, for numbers x and y; to show this we can show $x \leqslant y$ and $y \leqslant x$.

Proposition 3.18. *It is the case that* $\{a^2 \,:\, a \in \mathbb{R}\} = \{a \in \mathbb{R} \,:\, a \geqslant 0\}$.

Proof. Define $P = \{a \in \mathbb{R} \,:\, a \geqslant 0\}$ and $S = \{a^2 \,:\, a \in \mathbb{R}\}$.

Assume $x \in S$. Therefore $x = a^2$ for some real number a. We observe that $x = a^2 \geqslant 0$, and hence $x \in \mathbb{R}$ and $x \geqslant 0$. Thus, by definition $x \in P$. Since $x \in S$ implies $x \in P$, we have shown $S \subseteq P$.

Next, assume $x \in P$. Therefore x is a non-negative real number. Consider $a = \sqrt{x} \in \mathbb{R}$, then $x = (\sqrt{x})^2 = a^2$. Hence, by definition $x \in S$. Since $x \in P$ implies $x \in S$, we have shown $P \subseteq S$.

We have shown $S \subseteq P$ and $P \subseteq S$, and thus we conclude $\{a^2 \,:\, a \in \mathbb{R}\} = \{a \in \mathbb{R} \,:\, a \geqslant 0\}$. □

3.4. Set Operations

Definition 3.19 (Unions and Intersections)**.** Given two sets A and B,

- the **union** of A and B is the set

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

- the **intersection** of A and B is the set

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

Consider a collection of sets $A_1, A_2, \ldots, A_n$,

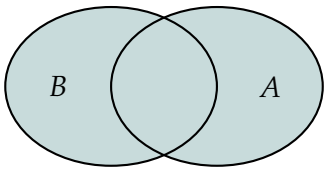
- The union of all of these sets is the set

$$A_1 \cup A_2 \cup \cdots \cup A_n = \{x \,:\, x \in A_i \text{ for some } i\} = \bigcup_{i=1}^{n} A_n$$

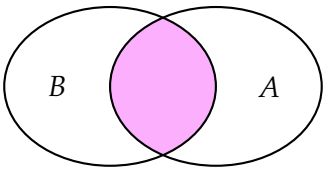
- The intersection of all these sets is the set

$$A_1 \cap A_2 \cap \cdots \cap A_n = \{x \,:\, x \in A_i \text{ for all } i\} = \bigcap_{i=1}^{n} A_n$$

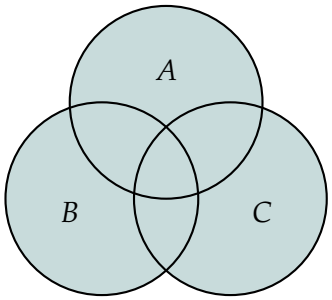
Discussion 3.20. A helpful way to visualise a collection of sets is via *Venn diagrams*. For example, below are $A \cup B$, $A \cap B$, $A \cup B \cup C$ and $A \cap B \cap C$, represented by the shaded region in the diagrams.



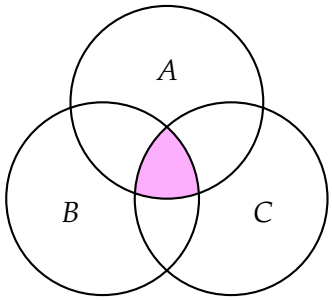
$A \cup B$



$A \cap B$



$A \cup B \cup C$



$A \cap B \cap C$

For numbers, the basic arithmetic operations are addition, subtraction and multiplication. Each of these has an analogous operation in set theory. For sets, these are union, which we have already introduced, *set difference* and *Cartesian product*.

Just as taking the absolute value of a number tells us how big it is, in set theory one can determine the size of a set by its *cardinality*.

We introduce all these notion in what comes next.

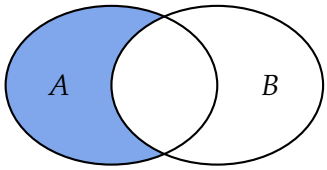
Lecture 9

Definition 3.21 (More Set Operations)**.** Given two sets A and B,

- the **difference** of B from A is the set

$$A \setminus B = \{x \in A \ : \ x \in A \text{ and } x \notin B\}$$

That is, it is the set that's left when we remove the part of B that belonged to A.

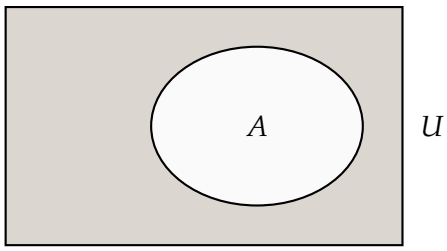


$A \setminus B$

- if $A \subseteq U$, for some set U, then U is called a *universal set* of A. The **complement** of A in U is the set

$$A^c = U \setminus A = \{x \in U \ : \ x \notin A\}$$

That is, it is the set of exactly those elements in U that don't belong to A.



A^c

⚠ The notion of a *complement of a set* A only make sense within the context of there being a universal set. Moreover, a set can different complements depending on different universal sets. For example, consider $A = \{0\}$, then a universal set of $\{0\}$ is $\{0\}$ itself, and the complement of $\{0\}$ in $\{0\}$ is $\varnothing$. Another universal set of $\{0\}$ is $\mathbb{R}$, and the complement of $\{0\}$ in $\mathbb{R}$ is the set of non-zero real numbers.

Example 3.22. Let A be the set of odd integers, and let B be the set of even integers.

- What is $A \cup B$? $A \cap B$? $\mathbb{Z} \setminus A$? $A \setminus B$?
- If $\mathbb{Z}$ is the universal set, then $A^c = B$, $B^c = A$, $\mathbb{Z}^c = \varnothing$ and $\varnothing^c = \mathbb{Z}$.

Definition 3.23 (Power Set & Cardinality)**.** Given a set A,

- the **power set** of A is the set $\mathcal{P}(A) = \{X \ : \ X \subseteq A\}$.
- the **cardinality** of A is the number of elements in A, and is denoted $|A|$.

Remark 3.24. The power set of A is denoted $\mathcal{P}(A)$, and it itself is a set. What are its elements? We first observe that every element of $\mathcal{P}(A)$ is itself a set. Which sets are elements of $\mathcal{P}(A)$? Those that are the subsets of A. That is, if X is a *subset of* A, then X is an *element of* $\mathcal{P}(A)$. For example, $A \in \mathcal{P}(A)$ and $\varnothing \in \mathcal{P}(A)$.

Example 3.25.

- Let $A = \{1, 2, 3\}$, so $|A| = 3$.

$$\varnothing \subseteq A$$

$$1 \in A, \text{ so } \{1\} \subseteq A$$

$$1,\ 2 \in A, \text{ so } \{1, 2\} \subseteq A$$

$$1,\ 2,\ 3 \in A, \text{ so } A = \{1, 2, 3\} \subseteq A$$

  We then get

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

- The power set $\mathcal{P}(\mathbb{Z})$ is the set of all sets consisting of integers. Every set which contains only integers, whether that be an infinite set like the set of all even integers, or finite like $\{-23, 17, -5\}$, is an element of $\mathcal{P}(\mathbb{Z})$. Also observe that $|\mathbb{Z}| = \infty$, i.e., it is not a finite set.
- What is the cardinality of $\{\{1, 2\}, \{a, b, c\}\}$?

We look at one final set operation, where we once again combine two sets to create a new set.

Definition 3.26 (Cartesian Product)**.** Given two sets A and B, the **Cartesian product** of A and B is the set

$$A \times B = \{(a, b) \ : \ a \in A \text{ and } b \in B\}$$

Example 3.27.

- Suppose $A = \{1, 2, 3\}$ and $B = \{\text{red}, \text{blue}\}$, then

$$A \times B = \{(1, \text{red}), (1, \text{blue}), (2, \text{red}), (2, \text{blue}), (3, \text{red}), (3, \text{blue})\}$$

The elements can be generated via a table:

B \ A	1	2	3
red	$(1, \text{red})$	$(2, \text{red})$	$(3, \text{red})$
blue	$(1, \text{blue})$	$(2, \text{blue})$	$(3, \text{blue})$

- Let $A = B = \mathbb{R}$, the set of all real numbers.

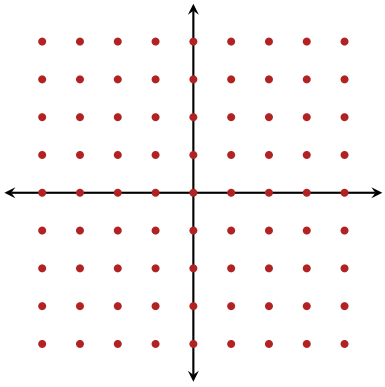
$$\mathbb{R} \times \mathbb{R} = \{(x, y) \ : \ x, y \in \mathbb{R}\}$$

Standard notation for this set is $\mathbb{R}^2$, the Euclidean (or Cartesian) plane.

- A subset of $\mathbb{R}^2$ is given by the set of all ordered pairs of integers

$$\mathbb{Z} \times \mathbb{Z} = \{(m, n) \ : \ m, n \in \mathbb{Z}\}$$

which can be plotted as



Proposition 3.28. *Suppose A and B are sets. If $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, then $A \subseteq B$.*

PROOF IDEA. Definitions!

Proof (Method 1). Let A and B be sets such that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$; we wish to prove that $A \subseteq B$. Consider $x \in A$, then $\{x\} \subseteq A$. By definition of the power set, we have $\{x\} \in \mathcal{P}(A)$. Since $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, we may deduce that $\{x\} \in \mathcal{P}(B)$. Therefore, we have $\{x\} \subseteq B$, and hence we may conclude that $x \in B$.

Since we have shown that $x \in A$ implies $x \in B$, and thus $A \subseteq B$. □

Proof (Method 2). Let A and B be sets such that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$; we wish to prove that $A \subseteq B$. Observe that since $A \subseteq A$, therefore by definition of the power set we have $A \in \mathcal{P}(A)$. By assumption, we have $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, and hence we deduce that $A \in \mathcal{P}(B)$. Thus, we may conclude that $A \subseteq B$, as we wished to prove. □

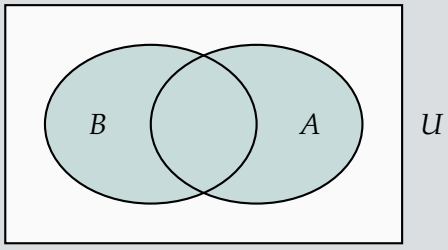
Lecture 10

Theorem 3.29 (De Morgan's Laws)**.** *Suppose A and B are subsets of a universal set U. Then,*

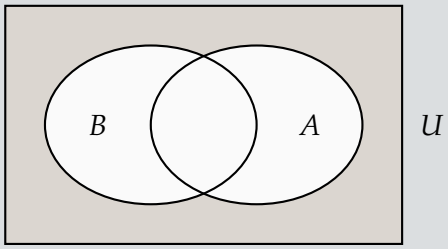
$$(A \cup B)^c = A^c \cap B^c \quad \textit{and} \quad (A \cap B)^c = A^c \cup B^c$$

SCRATCH WORK. We will prove the first identity, and leave the second as an exercise. We will try and make sense of the first identity using Venn diagrams, but they will not constitute a proof. Our proof will follow the proof strategy of proving set equality.

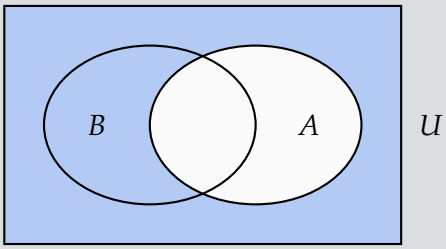
Let us start with $A \cup B$ in the set U

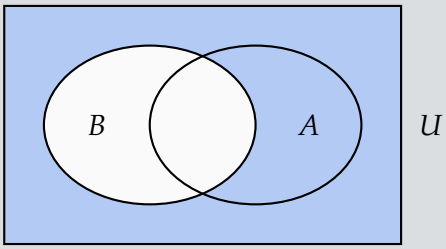


Taking the complement (in U) we get $(A \cup B)^c$, which is

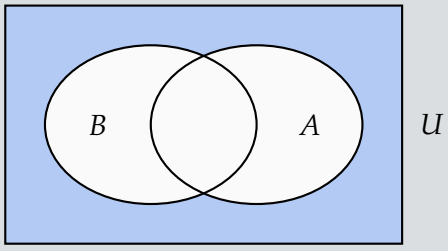


Let us now consider A^c and B^c





The Venn diagram of $A^c \cap B^c$ is the region shaded in both of the above diagrams, which is



This diagram is the same as the one for $(A \cup B)^c$ above!

Remark 3.30. Visualising using Venn diagrams gives on a way to imagine why given statements

involving sets could potentially be true, but they *do not* constitute a proof. To write proofs of set containment and set equality, we must use produce a proof that follows the outline laid out in Discussions 3.10 and 3.16.

Proof. We prove the first identity. Suppose A and B are subsets of a universal set U, we wish to prove that $(A \cup B)^c = A^c \cap B^c$.

We will first prove that $(A \cup B)^c \subseteq A^c \cap B^c$. Assume $x \in (A \cup B)^c$, then by definition of the complement we have $x \in U$ and

$$x \notin (A \cup B)$$

By definition of the union, x can be in neither in A nor B. Therefore,

$$x \notin A \quad \text{and} \quad x \notin B$$

which, by the definition of the complement, gives us

$$x \in A^c \quad \text{and} \quad x \in B^c$$

Hence, by the definition of the complement, we have

$$x \in A^c \cap B^c$$

We have shown that $x \in (A \cup B)^c$ implies $x \in A^c \cap B^c$, which means

$$(A \cup B)^c \subseteq A^c \cap B^c$$

We will next prove that $A^c \cap B^c \subseteq (A \cup B)^c$. Assume $x \in A^c \cap B^c$, then by definition of the intersection we have

$$x \in A^c \cap B^c$$

By definition of the complement, we have $x \in U$ and

$$x \in A^c \quad \text{and} \quad x \in B^c$$

Therefore, by definition of the union, we get

$$x \notin (A \cup B)$$

Hence, by the definition of the complement, we have

$$x \in (A \cup B)^c$$

We have shown that $x \in A^c \cap B^c$ implies $x \in (A \cup B)^c$, which means

$$A^c \cap B^c \subseteq (A \cup B)^c$$

Thus, having shown that

$$(A \cup B)^c \subseteq A^c \cap B^c \quad \text{and} \quad A^c \cap B^c \subseteq (A \cup B)^c$$

we conclude $(A \cup B)^c = A^c \cap B^c$. □

4. Induction

4.1. A Chain Reaction

Discussion 4.1. Suppose you are told by a friend that they have a set of dominoes, and they ask you under what conditions will the dominoes topple. The following seem like reasonable conditions, once one has set the dominoes in a row:

(1) If you give the first domino a push, it should fall.

(2) Moreover, any domino when it is knocked should fall and knocks the next one over.

Given these conditions, we know that when we push the first domino, the every domino will eventually fall. Why is that?

Our condition one tells us that when we push the first domino, it falls. Moreover, the second condition tells us that when the first domino falls, so does the second. Apply the second condition once again tells us that when the second domino falls, so does the third one. Once again applying the second condition once again tells us that when the third domino falls, so does the fourth one. So on and so forth; a chain reaction!

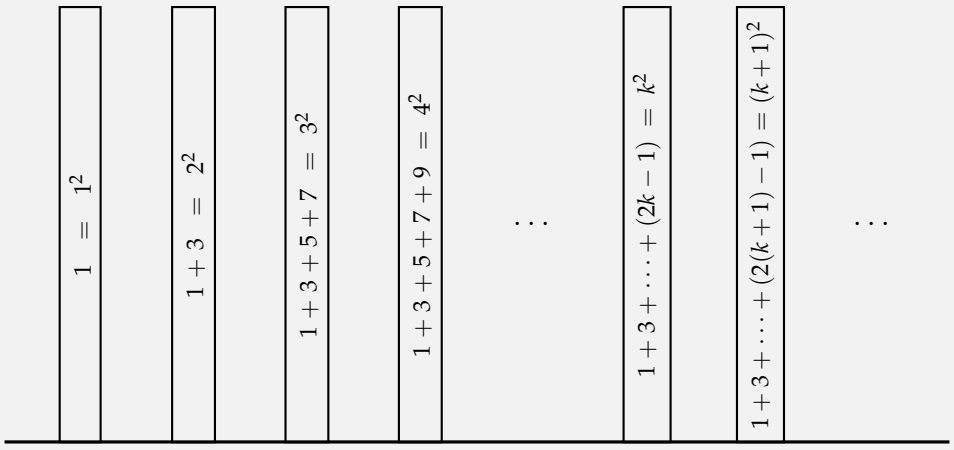
A similar thing works in mathematics. For example, take a look at the following

$$\begin{aligned} 1 &= 1 = 1^2 \\ 1+3 &= 4 = 2^2 \\ 1+3+5 &= 9 = 3^2 \\ 1+3+5+7 &= 16 = 4^2 \\ 1+3+5+7+9 &= 25 = 5^2 \\ 1+3+5+7+9+11 &= 36 = 6^2 \end{aligned}$$

Let us set-up our conjecture and see how the domino analogy allows us to imagine a proof strategy for the conjecture.

Conjecture 4.2. *Sum of the first n odd positive integers is n^2.*

How do we prove this is true for every one of the infinitely many n's? The trick is to use the domino idea. Imagine one domino for each of the above statements:



Suppose we do the following:

- Show that the first domino is true (this is trivial, since we clearly have $1 = 1^2$).
- Show that *any* domino, if true, implies that the following domino is true too.

Given these two, we may conclude that *all* the dominoes are true. This is a slick way to prove infinitely many statements all at once, and it is called the *principle of mathematical induction*, or, when among friends, it is simply called *induction*.

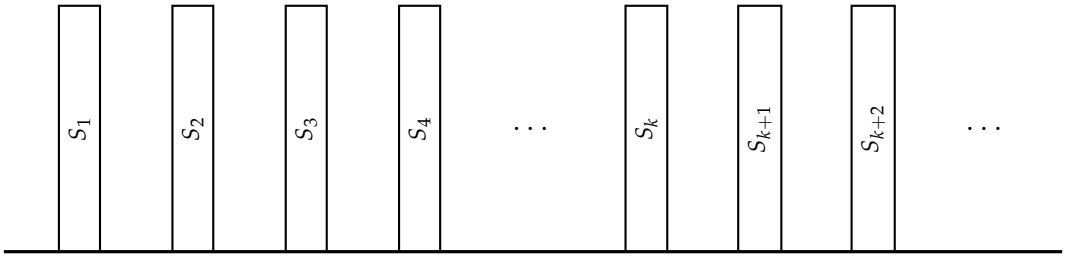
Lecture 11

Principle 4.3 (Principle of Mathematical Induction)**.** *Consider a sequence of mathematical statements S_1, S_2, S_3, ... The* Principle of **Induction** *states that*

- *suppose S_1 is true, and*
- *suppose, for each $k \in \mathbb{Z}_{>0}$, if S_k is true then S_{k+1} is true.*

Then, S_n is true for every $n \in \mathbb{Z}_{>0}$.

Discussion 4.4. This is modelled by the following picture.



The above suggests a general framework for how to use induction.

Proposition. S_1, S_2, S_3, ... are all true.

Proof. General set-up or assumptions, if needed. Declare that you are using induction.

Base Case. *Demonstrating that S_1 is true.*

Inductive Hypothesis. *Assuming that S_k is true.*

Inductive Step. *Proof that S_k implies S_{k+1}.*

Conclusion. Therefore, by induction, S_n is true for all integers $n \geqslant 1$. □

Remark 4.5. Another analogy that works is the analogy of a ladder. Assume there is a ladder that rests on the ground but climbs upwards forever.

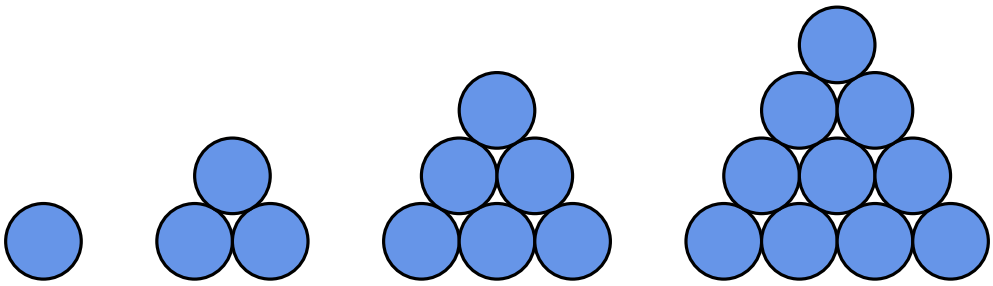
Assuming you can step on the first rung, and assuming that you can always step from one run to the next, then you can climb the ladder as high as possible! Maybe even forever!

4.2. Examples, examples, examples

We leave the example posed as Conjecture 4.2 as an exercise. We will see several examples that will illustrate this principle of induction.

Definition 4.6 (Triangular Numbers)**.** For a given positive integer n, we define the n^{th} **triangular number**, denoted T_n, to be

$$T_n = 1 + 2 + 3 + 4 + \cdots + n$$



Proposition 4.7. *For any $n \in \mathbb{Z}_{>0}$, the following is true*

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

PROOF IDEA. Since we discussed induction as a strategy to prove a series of statements indexed by positive integers. For any $n \in \mathbb{Z}_{>0}$, the n^{th} statement is

$$S_n : \ 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

To employ induction, we will first prove the statement

$$S_1 : \ 1 = \frac{1(1+1)}{2}$$

The right-hand side can be computed to be 1, and thus S_1 is a true statement. Let us now consider the k^{th} step: the statement S_k. That is, we *assume* that the following equation is true

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}$$

Here k is a fixed natural number, but we do not know what number it is. We wish to use the above equality and *prove* that the $(k+1)^{\text{th}}$ step

$$1 + 2 + 3 + \cdots + k + (k+1) = \frac{(k+1)((k+1)+1)}{2}$$

is true.

Proof. We proceed by induction to prove the statement

$$S_n : \ 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

for every $n \in \mathbb{Z}_{>0}$.

BASE CASE. The base case is $n = 1$, and

$$1 = \frac{2}{2} = \frac{1(1+1)}{2}$$

as we needed to show.

INDUCTIVE HYPOTHESIS. Let $k \in \mathbb{Z}_{>0}$, and assume that

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}$$

INDUCTIVE STEP. We aim to prove that the statement S_{k+1} is true. Let us start with the left-hand side

$$\begin{aligned}
1 + 2 + 3 + \cdots + k + (k+1) &= (1 + 2 + 3 + \cdots + k) + (k+1) \\
&= \frac{k(k+1)}{2} + (k+1) && \text{using the inductive hypothesis} \\
&= (k+1)\left(\frac{k}{2} + 1\right) \\
&= (k+1) \cdot \frac{k+2}{2} \\
&= \frac{(k+1)(k+2)}{2} \\
&= \frac{(k+1)((k+1)+1)}{2}
\end{aligned}$$

as desired.

Therefore, by induction, we have proven that

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

for every integer $n > 0$. □

Remark 4.8. Using this formula for T_n, for an integer $n > 0$, i.e.

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

We experiment and see what values $T_n + T_{n+1}$ give us for various n

n	T_n	T_{n+1}	$T_n + T_{n+1}$
1	1	3	4
2	3	6	9
3	6	10	16
4	10	15	25
5	15	21	36
6	21	28	49

It sure looks like $T_n + T_{n+1} = (n+1)^2$. Try using induction to prove this fact!

Proposition 4.9. *For an integer $n \geqslant 1$ and a real number $a \neq 1$, we have*

$$1 + a + \cdots + a^n = \frac{1 - a^{n+1}}{1 - a}$$

Proof. We proceed by induction to prove the statement

$$S_n : \ 1 + a + \cdots + a^n = \frac{1 - a^{n+1}}{1 - a}$$

for every $n \in \mathbb{Z}_{>0}$.

BASE CASE. The base case is $n = 1$. The left-hand side in the statement S_1 is $1 + a$, while the right-hand side is

$$\frac{1 - a^2}{1 - a} = \frac{(1 - a)(1 + a)}{1 - a} = 1 + a$$

since $1 - a \neq 0$. Therefore

$$1 + a = \frac{1 - a^2}{1 - a}$$

as we needed to show.

INDUCTIVE HYPOTHESIS. Let $k \in \mathbb{Z}_{>0}$, and assume that

$$1 + a + \cdots + a^k = \frac{1 - a^{k+1}}{1 - a}$$

INDUCTIVE STEP. We aim to prove that the statement S_{k+1} is true. That is, we wish to show that

$$1 + a + \cdots + a^k + a^{k+1} = \frac{1 - a^{k+2}}{1 - a}$$

Let us start with the left-hand side

$$\begin{aligned}
1 + a + \cdots + a^k + a^{k+1} &= (1 + a + \cdots + a^k) + a^{k+1} \\
&= \frac{1 - a^{k+1}}{1 - a} + a^{k+1} && \text{using the inductive hypothesis} \\
&= \frac{1 - a^{k+1}}{1 - a} + \frac{a^{k+1}(1 - a)}{1 - a} \\
&= \frac{1 - a^{k+1} + (a^{k+1} - a^{k+2})}{1 - a} \\
&= \frac{1 - a^{k+2}}{1 - a}
\end{aligned}$$

as desired.

Therefore, by induction, we have proven that

$$1 + a + \cdots + a^n = \frac{1 - a^{n+1}}{1 - a}$$

for every integer $n > 0$. □

Remark 4.10. Re-writing the equality in Proposition 4.9 as

$$1 - a^{n+1} = (1-a)(1 + a + \cdots + a^n) \tag{⚗}$$

this is now true for $a = 1$ as well. So (⚗) is true for all real numbers a.

If we write $a = y/x$ for real numbers x, y, where $x \neq 0$, we get

$$1 - (y/x)^{n+1} = (1 - (y/x))(1 + (y/x) + \cdots + (y/x)^n)$$

Multiplying both sides by x^n, we get

$$x^{n+1} - y^{n+1} = (x-y)(x^n + x^{n-1}y + \cdots + xy^{n-1} + y^n)$$

One can now verify that this equality is *also* true for $x = 0$. Hence, the above expression is true for all pairs of real numbers.

Lecture 12

Proposition 4.11. *For every integer $n \geqslant 1$, the product of the first n odd numbers equals $\dfrac{(2n)!}{2^n n!}$. That is,*

$$1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1) = \frac{(2n)!}{2^n n!}$$

Proof. We proceed by induction to prove the statement

$$S_n : \ 1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1) = \frac{(2n)!}{2^n n!}$$

for every $n \in \mathbb{Z}_{>0}$.

BASE CASE. The base case is $n = 1$. The left-hand side in the statement S_1 is 1, while the right-hand side is

$$\frac{2!}{2^1 \cdot 1!} = \frac{2}{2} = 1$$

Therefore

$$1 = \frac{2!}{2^1 \cdot 1!}$$

as we needed to show.

INDUCTIVE HYPOTHESIS. Let $k \in \mathbb{Z}_{>0}$, and assume that

$$1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2k-1) = \frac{(2k)!}{2^k k!}$$

INDUCTIVE STEP. We aim to prove that the statement S_{k+1} is true. That is, we wish to show that

$$\begin{aligned} 1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2k-1) \cdot (2k+1) &= \frac{(2(k+1))!}{2^{k+1}(k+1)!} \\ &= \frac{(2k+2)!}{2^{k+1}(k+1)!} \end{aligned}$$

Let us start with the left-hand side

$$\begin{aligned}
1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2k-1) \cdot (2k+1) &= (1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2k-1)) \cdot (2k+1) \\
&= \frac{(2k)!}{2^k k!} \cdot (2k+1) && \text{using the inductive hypothesis} \\
&= \frac{(2k+1)!}{2^k k!} \\
&= \frac{(2k+1)!}{2^k k!} \cdot \frac{2k+2}{2k+2} \\
&= \frac{(2k+2)!}{2^k k! \cdot (2k+2)} \\
&= \frac{(2k+2)!}{2^k k! \cdot 2 \cdot (k+1)} \\
&= \frac{(2k+2)!}{2^{k+1}(k+1)!}
\end{aligned}$$

as desired.

Therefore, by induction, we have proven that

$$1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1) = \frac{(2n)!}{2^n n!}$$

for every integer $n > 0$. □

4.3. Strong Induction

Discussion 4.12. The idea behind the variation of induction, that we wish to introduce, is that at the point when the 100^{th} domino is the next to get knocked down, you know for sure that all of the first 99 dominoes have fallen, not just 99^{th} one.

Likewise, when you are proving some sequence of statements S_1, S_2, S_3, . . ., instead of assuming only S_k to be true to prove S_{k+1}, why not assume that S_1, S_2, . . . , S_k are *all* true to prove S_{k+1}? After all, by the time we are proving S_{k+1}, the statements S_1, S_2, . . . , S_k must already have been shown to be true!

Principle 4.13 (Principle of Strong (Mathematical) Induction)**.** *Consider a sequence of mathematical statements S_1, S_2, S_3, ... The* Principle of **Strong Induction** *states that*

- *suppose S_1 is true, and*
- *suppose, for any $k \in \mathbb{Z}_{>0}$, if $S_1, S_2, \ldots, S_k$ are all true, then S_{k+1} is true.*

Then, S_n is true for every $n \in \mathbb{Z}_{>0}$.

Discussion 4.14. The general framework of writing a proof by strong induction is similar to the one for induction we provided in Discussion 4.4.

Proposition. S_1, S_2, S_3, ... are all true.

Proof. General set-up or assumptions, if needed. Declare that you are using strong induction.

Base Case. *Demonstrating that S_1 is true.*

Inductive Hypothesis. *Assuming that $S_1, S_2, \ldots, S_k$ are all true.*

Inductive Step. *Proof that $S_1, S_2, \ldots, S_k$ implies S_{k+1}.*

Conclusion. Therefore, by (strong) induction, S_n is true for all integers $n \geqslant 1$. □

Remark 4.15 (A General Base Case)**.** Until now we have been discussing methods of proof for a sequence of statements whose index starts at 1, i.e., sequences of the form $S_1, S_2, S_3, \ldots$.

It is possible to be handed a sequence of statements, where it makes sense to index them with an integer b other than 1, i.e., a sequence of statements of the form $S_b, S_{b+1}, S_{b+1}, \ldots$. In this case, one can still use induction to provide a proof of this sequence of statements. The base case will now be S_b, the *first statement* in the sequence of statements that you are attempting prove.

The proof-writing framework to prove this sequence of statements will look like the following; the framework for strong induction will be similar. Here $b \in \mathbb{Z}$.

Proposition. S_b, S_{b+1}, S_{b+2}, ... are all true.

Proof. General set-up or assumptions, if needed. Declare that you are using strong induction.

Base Case. *Demonstrating that S_b is true.*

Inductive Hypothesis. *For any $k \in \mathbb{Z}$ with $k \geqslant b$, assume that S_k is true.*

Inductive Step. *Proof that S_k implies S_{k+1}.*

Conclusion. Therefore, by (strong) induction, S_n is true for all integers $n \geqslant b$. □

Theorem 4.16 (Fundamental Theorem of Arithmetic)**.** *Every integer $n \geqslant 2$ is either a prime or a product of primes. Furthermore, this prime decomposition is unique.*

PROOF IDEA. We wish to prove the statement

$$S_n : \quad n \text{ is either a prime or a product of primes}$$

for any $n \geqslant 2$. That is, we wish to prove the sequence of statements $S_2, S_3, S_4, \ldots$. Therefore, our base case is when $n = 2$, i.e., it is showing that S_2 is true. Which it is!

We will use strong induction in this proof, therefore let us assume that we have shown the statements $S_2, S_3, \ldots, S_k$ are all true, i.e., we are assuming that all integers $2 \leqslant a \leqslant k$ are either primes or a product of primes.

We wish to prove that $k + 1$ is either a prime or a product of primes. If it a prime, then we're

done! So, let us assume that $k+1$ is not a prime, that is, it is a composite number. In this case

$$k+1 = st, \quad \text{where } 1 \leqslant s, t \leqslant k.$$

Hence s, t are in the range of integers to which we may apply the inductive hypothesis, so s and t are either primes of product of primes, then st is necessarily a product of primes.

Proof. We prove the statement using strong induction.

BASE CASE. The base case is $n = 2$, and since 2 itself is a prime, we are done.

INDUCTIVE HYPOTHESIS. Let k be an integer such that $k \geqslant 2$, and we assume that each of the integers $2, 3, \ldots, k$ is either a prime or a product of primes.

INDUCTIVE STEP. We aim to prove $k+1$ is a prime or a product of primes. Since $k+1 > 2$, it is either a prime or composite. We will consider both cases.

Case 1. Assume $k+1$ is prime. Since our aim is to show $k+1$ is either a prime or product of primes, so $k+1$ being prime means we have achieved our aim. Therefore, we are done.

Case 2. Assume $k+1$ is composite. Then, by Definition 2.29, we may write

$$k+1 = st, \quad \text{where } 1 < s, t < k+1.$$

Therefore

$$2 \leqslant s \leqslant k \quad \text{and} \quad 2 \leqslant t \leqslant k$$

By the inductive hypothesis, we may write s and t as a product of primes

$$s = p_1 \cdot p_2 \cdot \ldots \cdot p_m \quad \text{and} \quad s = q_1 \cdot q_2 \cdot \ldots \cdot q_\ell$$

where $m, \ell \geqslant 1$ are integers. Hence,

$$k+1 = st = (p_1 \cdot p_2 \cdot \ldots \cdot p_m) \cdot (q_1 \cdot q_2 \cdot \ldots \cdot q_\ell)$$

is also a product of primes.

Thus, $k+1$ is either a prime or a product of primes.

Therefore, by induction, every integer $n \geqslant 2$ is either a prime or a product of primes. □

Proposition 4.17. *Every integer $n \geqslant 11$ can be written $2a + 5b$ for some positive integers a and b.*

PROOF IDEA. We observe that our base case will be when $n = 11$. Let us try and write 11 as $2a + 5b$ for some positive integers a and b. Seems like $a = 3$ and $b = 1$ work

$$11 = 2 \cdot 3 + 5 \cdot 1$$

It is not clear how this can help us write 12 as $2a + 5b$ for some positive integers a, b. Why don't we try and write down a few numbers in this form

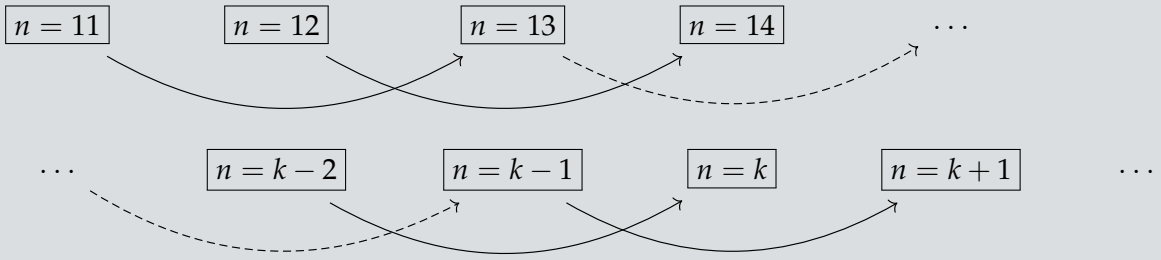
- $11 = 2 \cdot 3 + 5 \cdot 1$
- $13 = 2 \cdot 4 + 5 \cdot 1$
- $15 = 2 \cdot 5 + 5 \cdot 1$
- $12 = 2 \cdot 1 + 5 \cdot 2$
- $14 = 2 \cdot 2 + 5 \cdot 2$
- $16 = 2 \cdot 3 + 5 \cdot 2$

Writing our examples is the best way to figure out what a proof could look like. Are there any interesting patterns that we notice here? Say, for the expression for 11 and 13, or for 12, 14 or 16?

To go from the $n = 14$ case to the $n = 16$ case, for example, all we need to is add 2, in which case $2 \cdot \mathbf{2} + 5 \cdot 2$ turns into $2 \cdot \mathbf{3} + 5 \cdot 2$.

This is how we will prove the given statement; each case relies on two previous cases. How do we prove the $n = k + 1$ case? Well, we will use the $n = k - 1$ case, which we will have assumed to be true under the inductive hypothesis.

But to make this strong induction argument, we will have to exhibit *two* base cases; since the inductive chain reaction is of the following form:



That is, in our induction step to prove $k + 1$ we require both k and $k - 1$ to be true.

Lecture 13

Proof. We prove the statement using strong induction.

BASE CASE. The base case is $n = 11$ and $n = 12$, since in the induction step we need two cases prior. Both these numbers can be expressed as asserted:

$$11 = 2 \cdot 3 + 5 \cdot 1$$
$$12 = 2 \cdot 1 + 5 \cdot 2$$

INDUCTIVE HYPOTHESIS. Let k be an integer such that $k \geqslant 11$, and we assume the result holds for $n = 2, 3, \ldots, k$.

INDUCTIVE STEP. We aim to prove the result for $n = k + 1$. By the inductive hypothesis,

$$k - 1 = 2a + 5b$$

for some positive integers a and b. Then, we have

$$k + 1 = (k - 1) + 2 = (2a + 5b) + 2 = 2(a + 1) + 5b$$

Since a is a positive integers, so is $a + 1$, and we already know b to be a positive integer. Thus, the above expression is indeed the desired representation of $k + 1$.

Therefore, by induction, every integer $n \geqslant 11$ can be written as the proposition asserts. □

Remark 4.18 (Multiple Base Cases)**.** In Proposition 4.17 above, we saw that the $(k+1)^{\text{th}}$ case within the induction step, required us to explicitly assume the k^{th} and $(k-1)^{\text{th}}$ step. This is contrasted with Theorem 4.16, where we were not really sure which previous cases did the $(k+1)^{\text{th}}$ case depends on.

Like in the case of the proposition, if we explicitly know the previous cases we must rely on, maybe there are two previous cases, then that is analogous to saying that it takes the previous *two* dominoes to knock over the next one. Thus, if we now the 1^{st} and 2^{nd} domino, then they will collectively knock the 3^{rd}. Then, since the 2^{nd} and 3^{rd} dominoes have fallen, this will knock the 4^{th} one. Then the 3^{rd} and 4^{th} will knock the 5^{th} one; and so on. Thus, this induction process, explicitly relies on two base cases, since without knocking the first two, the third won't fall, and the chain reaction will not begin.

In the same way, if each step relies on previous three steps, then you must prove three base cases. If each step relies on previous four, then you must prove four base cases. And so on. But, fortunately, in practice, things rarely get this crazy.

4.4. Non-examples

A small error in reasoning in an induction proof allows us to "prove" all sorts of ridiculous things!

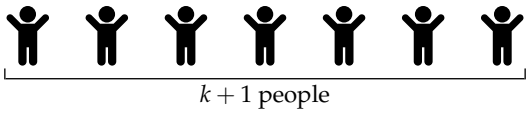
***Faux Proposition* 1.** *Everyone on Earth has the same name.*

"Proof". We will consider groups of n people at a time, and by induction we will "prove" that for every positive integer n, every group of n people must have everyone with the same name.

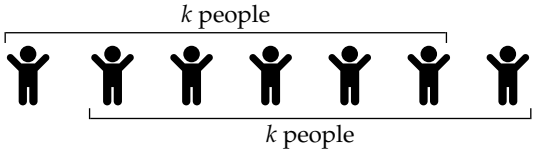
BASE CASE. If $n = 1$, then everyone in the group has the same name, since there's only one person in the group!

INDUCTIVE HYPOTHESIS. Let k be a positive integer, and assume that any group of k people all have the same name.

INDUCTIVE STEP. Consider a group of $k+1$ people



But notice that we can group the first k-many people, and also group the last k-many people, and apply the inductive hypothesis to these two groups:



Therefore these two groups have the same names, and hence the group of $(k+1)$-many people have the same name.

This "proves" by induction that for every positive integer n, every group of n people must have the same name. So, if you let $n =$ *number of people on Earth*, this "proves" everyone has the same name.

What is the error in *Faux Proposition* 1?

To find the mistake, try repeating the argument in the inductive step to go from the $n = 1$ case to $n = 2$ case!

***Faux Proposition* 2.** *The harmonic series converges. That is,*

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots < \infty$$

The notation $x < \infty$ is used to indicate that the number on the left, x, is a finite number.

"Proof". We "prove" this result using induction. We will let S_n be the statement

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots < \infty$$

BASE CASE. If $n = 1$, then of course $1 < \infty$. Therefore S_1 is true.

INDUCTIVE HYPOTHESIS. For a positive integer k, assume that

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k} < \infty$$

INDUCTIVE STEP. By the inductive hypothesis, $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k}$ is a finite number, let

$$F = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k}$$

Then,

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k+1} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k} + \frac{1}{k+1} = F + \frac{1}{k+1}$$

Since a finite number plus another finite number is finite, therefore $F + \frac{1}{k+1}$ is finite, and hence

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k+1} < \infty$$

This "proves" by induction that

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots < \infty$$

completing the "proof". 🐞

What is the error in *Faux Proposition* 2?

To find the mistake, think about what conclusion is actually being reached by the first three stages of the proof.

5. Logic

5.1. Statements

Lecture 14

Logic for us will be a way to organise of our mathematical thought and language.

Definition 5.1 (Statements)**.** A **statement** is a sentence or mathematical expression which can be objectively determined to be either *true* or *false*.

By sentence we mean a traditional sentence in English or another language one uses to communicate.

Example 5.2. Here are some examples of statements

- $\sqrt{2} \in \mathbb{R}$ (a *true* statement)
- $\sqrt{2} \in \mathbb{Z}$ (a *false* statement)
- $2 + 3 = 5$ (a *true* statement)
- $3 + 4 = 15$ (a *false* statement)
- all polynomials are continuous (a *true* statement)
- all integers are even (a *false* statement)

The following are *not* statements

- $8 + 9$
- $x + 7$
- $\mathbb{Q}$
- are polynomials differentiable?

Definition 5.3 (Open Sentences)**.** An **open sentence** is a sentence or mathematical expression which

- do not have a truth value,
- depend on some unknown, like a variable x or an arbitrary function f, and
- when the unknown specified, the sentence becomes a statement and so has a truth value. The truth value may depend on the value of the unknown one chooses.

Example 5.4. Here are some examples of open sentences

(i) $x + 7 = 12$

(ii) $3 \mid n$

(iii) f is continuous

(iv) m is even

Note that

- (i) is *true* when $x = 5$ but *false* for any $x \neq 5$.
- (ii) is *true*, e.g., when $n = 6$ but *false*, e.g., for $n = 7$.

Remark 5.5. We use upper-case letter $P, Q, R, \ldots$ to denote statements. Open sentences are often written similarly, or perhaps like $P(x), Q(n), R(f), \ldots$ if one wishes to emphasise the unknown.

Notation 5.6 (And, Or, Negation)**.** Let P and Q be statements or open sentences.

- $P \wedge Q$ is the statement "*P and Q*", and is called the **conjunction**.
- $P \vee Q$ is the statement "*P or Q*", and is called the **disjunction**.
- $\neg P$ is the statement "*not P*", and is called the **negation** of P.

Example 5.7. Consider the following statements

- P : 3 is odd
  This is *true*.
- Q : 4 is even
  This is *true*.
- R : 5 is even
  This is *false*.
- S : 6 is odd
  This is *false*.

Then,

- $P \wedge Q$: 3 is odd and 4 is even
  This is *true*.

  $P \wedge R$: 3 is odd and 5 is even
  This is *false*.
- $P \vee R$: 3 is odd or 5 is even
  This is *true*.

  $R \vee S$: 5 is even or 6 is odd
  This is *false*.
- $\neg P$: 3 is not odd
  This is *false*.

  $\neg S$: 6 is not odd
  This is *true*.
- $P \wedge \neg Q$: 3 is odd and 4 is not even
  This is *false*.

  $S \vee \neg S$: 6 is odd or 6 is not odd
  This is *true*.

Notation 5.8 (Implication, Biconditional)**.** Let P and Q be statements or open sentences.

- $P \Rightarrow Q$ is the statement "*P implies Q*", and is called the **implication**.
- $P \Leftrightarrow Q$ is the statement "*P if and only if Q*", and is called the **biconditional**.

Discussion 5.9 (Reading Implication)**.** The statement $P \Rightarrow Q$ is read in several different ways, not including *P implies Q*.

$$\left.\begin{array}{r} \textit{if } P\textit{, then } Q \\ Q \textit{ if } P \\ P \textit{ only if } Q \\ Q \textit{ whenever } P \\ P \text{ is } \textit{sufficient} \text{ for } Q \\ Q \text{ is } \textit{necessary} \text{ for } P \end{array}\right\} \text{all mean } P \Rightarrow Q$$

Discussion 5.10 (Reading Biconditional)**.** The statement $P \Leftrightarrow Q$ is read in several different ways, not including *P if and only if Q*.

$$\left.\begin{array}{l} P \text{ is equivalent to } Q \\ P \text{ is necessary and sufficient for } Q \\ P \text{ implies } Q \text{ and } Q \text{ implies } P \\ \text{if } P\text{, then } Q\text{, and conversely} \\ \text{Shorthand: } P \text{ iff } Q \\ \text{Symbolic: } (P \Rightarrow Q) \wedge Q \Rightarrow P \end{array}\right\} \text{all mean } P \Leftrightarrow Q$$

Definition 5.11 (Converse)**.** The **converse** of the implication $P \Rightarrow Q$ is the implication $Q \Rightarrow P$.

Remark 5.12. If $P \Rightarrow Q$ is true, it is not necessarily the case that $Q \Rightarrow P$ is true. For example,

$$\text{if } x = 2\text{, then } x \text{ is even}$$

is certain a true statement. But

$$\text{if } x \text{ is even, then } x = 2$$

is false.

Discussion 5.13 (Intuition from Set Theory)**.** There is a certain dictionary between set operations and logical connectives. We leave it to the reader to dig deeper.

$P \vee Q$	$A \cup B$
$P \wedge Q$	$A \cap B$
$\neg P$	A^c
$P \Rightarrow Q$	$A \subseteq B$
$P \Leftrightarrow Q$	$A = B$

5.2. Truth Tables

Lecture 15

A *truth table* models the relationship between the truth values of different statements.

Discussion 5.14. Let P and Q be statements. Let us consider the truth tables for the connectives in Notation 5.6

- The *negation* of P is the statement *not* P. Its truth table is:

P	$\neg P$
T	**F**
F	**T**

- The *disjunction* of P and Q is the statement P *or* Q. Its truth table is:

P	Q	$P \vee Q$
T	**T**	**T**
T	**F**	**T**
F	**T**	**T**
F	**F**	**F**

- The *conjunction* of P and Q is the statement P *and* Q. Its truth table is:

P	Q	$P \vee Q$
T	**T**	**T**
T	**F**	**F**
F	**T**	**F**
F	**F**	**F**

Definition 5.15 (Tautology and Contradiction)**.** A statement is called a **tautology** if it is *true* for all possible combinations of truth values of its component statements. We denote any tautology as $\top$.

A statement is called a **contradiction** if it is *false* for all possible combinations of truth values of its component statements. We denote any contradiction as $\bot$.

Example 5.16.

(1) $P \vee (\neg P)$ is a tautology.

P	$\neg P$	$P \vee (\neg P)$
T	**F**	**T**
F	**T**	**T**

(2) $P \wedge (\neg P)$ is a contradiction.

P	$\neg P$	$P \wedge (\neg P)$
T	**F**	**F**
F	**T**	**F**

Definition 5.17 (Logical Equivalence)**.** Two statements R and S are **logically equivalent** if they have the same truth value for all possible combinations of truth values of its component statements. We denote this as $R \equiv S$.

R and S are logically equivalent if and only if the biconditional statement $R \Leftrightarrow S$ is a tautology.

Theorem 5.18 (Laws of Logical Equivalence)**.** *Let P, Q and R be statements, and let $\top$ and $\bot$ be a tautology and contradiction respectively, then*

(L1) Identity laws

$$P \vee \bot \equiv P$$

$$P \wedge \top \equiv P$$

(L2) Domination laws

$$P \vee \top \equiv \top$$

$$P \wedge \bot \equiv \bot$$

(L3) Double Negation law

$$\neg(\neg P) \equiv P$$

(L4) Commutative laws

$$P \vee Q \equiv Q \vee P$$

$$P \wedge Q \equiv Q \wedge P$$

(L5) Associative laws

$$P \vee (Q \vee R) \equiv (P \vee Q) \vee R$$

$$P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$$

(L6) Distributive laws

$$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$$

$$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$$

(L7) De Morgan's laws

(L7a) $\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$

(L7b) $\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$

Proof. We simply have to build the appropriate truth tables. For example, for (L7a) we have

P	Q	$P \vee Q$	$\neg(P \vee Q)$	$\neg P$	$\neg Q$	$(\neg P) \wedge (\neg Q)$
T	**T**	**T**	**F**	**F**	**F**	**F**
T	**F**	**T**	**F**	**F**	**T**	**F**
F	**T**	**T**	**F**	**T**	**F**	**F**
F	**F**	**F**	**T**	**T**	**T**	**T**

Comparing the truth values, we see $\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$. □

Discussion 5.19. Let P and Q be statements. Let us consider the truth tables for the connectives in Notation 5.8

- Given the *implication* $P \Rightarrow Q$, the statement P is called the *hypothesis*, while Q is called the is *conclusion*. Its truth table is:

P	Q	$P \Rightarrow Q$
T	**T**	**T**
T	**F**	**F**
F	**T**	**T**
F	**F**	**T**

When hypothesis P is not satisfied ($\mathbf{F}$), then whatever the conclusion Q may be ($\mathbf{T}, \mathbf{F}$), the implication $P \Rightarrow Q$ is true.

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$
T	**T**	**T**	**T**	**T**
T	**F**	**F**	**T**	**F**
F	**T**	**T**	**F**	**F**
F	**F**	**T**	**T**	**T**

Note that $P \Leftrightarrow Q$ is true only when both P and Q are true or false.

Theorem 5.20. *Let P and Q be statements, then*

$$(P \Rightarrow Q) \equiv ((\neg P) \vee Q)$$

Proof. We build the truth table and compare the truth values.

P	Q	$\neg P$	$P \Rightarrow Q$	$(\neg P) \vee Q$
T	**T**	**F**	**T**	**T**
T	**F**	**F**	**F**	**F**
F	**T**	**T**	**T**	**T**
F	**F**	**T**	**T**	**T**

So comparing the truth values of $P \Rightarrow Q$ and $(\neg P) \vee Q$ we see $(P \Rightarrow Q) \equiv ((\neg P) \vee Q)$. □

5.3. Quantifiers and Negations

Lecture 16

Discussion 5.21 (Quantifiers)**.** Let $P(x)$ be an open sentence. Recall that $P(x)$ becomes a statement once we specify an x. We can produce specific kinds of statements from this open sentence called **quantified statements**.

One may specify a set S from which we allowed choose values for x.

- *for all $x \in S$, $P(x)$ is true.*

  The phrase "for all" is called **universal quantifier** and is denoted by the symbol $\forall$. Other ways to express the universal quantifier are "for every", "for any" and "for each".

  Symbolically, we express the universally quantified statement as

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

  The statement is true if $P(x)$ is true for every $x \in S$.

- *there exists $x \in S$ such that $P(x)$ is true.*

  The phrase "there exists" is called the **existential quantifier** and is denoted by the symbol $\exists$. Symbolically, we express the existentially quantified statement as

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

  The statement is true if $P(x)$ is true for at least one $x \in S$.

Example 5.22. Consider the open sentence

$$P(n) : n^2 + n \text{ is even}$$

with domain $\mathbb{Z}$, the set of integers. Then, we have statements

$$\text{for all } n \in \mathbb{Z},\ n^2 + n \text{ is even.} \qquad \forall n \in \mathbb{Z},\ P(n) \qquad (\mathbf{T})$$

$$\text{there exists an } n \in \mathbb{Z} \text{ such that } n^2 + n \text{ is even.} \qquad \exists n \in \mathbb{Z},\ P(n) \qquad (\mathbf{T})$$

Discussion 5.23 (Negation of Quantified Statements)**.**

$$\begin{aligned}\neg(\forall x \in S,\ P(x)) &= \text{it is not the case that for all } x \in S,\ P(x) \text{ is true.}\\ &= \text{there exists } x \in S \text{ such that } P(x) \text{ is false.}\\ &= \exists x \in S,\ \neg P(x)\end{aligned}$$

$$\begin{aligned}\neg(\exists x \in S,\ P(x)) &= \text{it is not the case that there exists } x \in S \text{ such that } P(x) \text{ is true.}\\ &= \text{for all } x \in S,\ P(x) \text{ is false.}\\ &= \forall x \in S,\ \neg P(x)\end{aligned}$$

Discussion 5.24 (Summarising Negation Rules)**.**

$$\text{under negation} \begin{cases} \wedge \leftrightarrow \vee \\ \forall \leftrightarrow \exists \\ P(x) \leftrightarrow \neg P(x) \end{cases}$$

Discussion 5.25 (Double Quantifiers and their Negation)**.** Let $x \in S$ and $y \in T$ be variables. Consider,

$$\forall x \in S,\ \forall y \in T,\ P(x,y)$$

for all $x \in S$ and $y \in T$, $P(x,y)$ is true.

The negation is

$$\begin{aligned}\neg(\forall x \in S,\ \forall y \in T,\ P(x,y)) &\equiv \exists x \in S, \neg(\forall y \in T,\ P(x,y))\\ &\equiv \exists x \in S,\ \exists y \in T,\ \neg P(x,y)\end{aligned}$$

For example, consider the statement *for all* $x \in \mathbb{R}$ *and* $y \in \mathbb{R}$, $x^2 + y^2 > 0$.

$$\text{Negation: } \textit{there exists } x \in \mathbb{R} \textit{ and } y \in \mathbb{R} \textit{ such that } x^2 + y^2 \leqslant 0.$$

This is **T**, since for $x = y = 0$ we have $x^2 + y^2 = 0$.

Similarly,

$$\begin{aligned}\neg(\forall x \in S,\ \exists y \in T,\ P(x,y)) &\equiv \exists x \in S, \neg(\exists y \in T,\ P(x,y)) \\ &\equiv \exists x \in S,\ \forall y \in T,\ \neg P(x,y)\end{aligned}$$

In other words,

$$\begin{aligned}&\neg(\text{for all } x \in S, \text{ there exists } y \in T \text{ such that } P(x,y) \text{ is true}) \\ &\qquad \equiv \text{there exists } x \in S \text{ such that for all } y \in T,\ P(x,y) \text{ is true}\end{aligned}$$

Finally,

$$\neg(\exists x \in S,\ \forall y \in T,\ P(x,y)) \equiv \forall x \in S,\ \exists y \in T,\ \neg P(x,y)$$

$$\neg(\exists x \in S,\ \exists y \in T,\ P(x,y)) \equiv \forall x \in S,\ \forall y \in T,\ \neg P(x,y)$$

Lecture 17

Discussion 5.26 (Negation of Implication)**.** If P and Q are statements, recall that $P \wedge Q$, $P \vee Q$ and $P \Rightarrow Q$ are statements too. We have discussed negating the former two, using De Morgan's laws (Theorem 5.18. Let us now discuss negating the implication. What is $\neg(P \Rightarrow Q)$?

Recall from Theorem 5.20 that

$$(P \Rightarrow Q) \equiv (\neg U \vee V)$$

Therefore,

$$\begin{aligned}\neg(P \Rightarrow Q) &\equiv \neg(\neg P \vee Q) \\ &\equiv \neg(\neg P) \wedge \neg Q && \text{by De Morgan's Laws} \\ &\equiv P \wedge \neg Q && \text{by Double Negation Law}\end{aligned}$$

Therefore, (negation of $P \Rightarrow Q$) is (P and not Q)

Definition 5.27 (Contrapositive of an Implication)**.** The **contrapositive** an implication $P \Rightarrow Q$ is the statement $\neg Q \Rightarrow \neg P$.

Theorem 5.28. *Let P and Q be statements, then $(P \Rightarrow Q) \equiv (\neg Q \Rightarrow \neg P)$.*

Proof. We know now that the most optimal way to prove this is not via truth tables but by using logical equivalence laws.

$$\begin{aligned}\neg Q \Rightarrow \neg P &\equiv \neg(\neg Q) \vee \neg P && \text{by Theorem 5.20} \\ &\equiv Q \vee \neg P && \text{by Double Negation law} \\ &\equiv \neg P \vee Q && \text{by Commutative Laws} \\ &\equiv P \Rightarrow Q && \text{by Theorem 5.20}\end{aligned}$$

□

5.4. Proving Quantified Statements

Discussion 5.29 (Proofs of Universally Quantified Statements)**.** Consider a universally quantified statement

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

Is this true or false?

If you think it is true, *prove it* using various methods of proof like direct proof, and yet to discuss methods like proof by contrapositive or contradiction. In this case, one will choose an *arbitrary element* and prove the statement is true for this arbitrary element.

If you think it is false, then its negation

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

is true. Therefore to show falsehood, we need to exhibit an (at least one) element $x_0 \in S$ such that $P(x_0)$ is false (that is, $\neg P(x_0)$ is true). x_0 is the called a **counterexample** to the given statement. Counterexamples prove the falsehood of, or disprove, universally quantified statements.

Conjecture 5.30. *If p is prime, then $2^p - 1$ is prime.*

DISPROOF IDEA. Notice that even though we did not use the language "for all", this is still a universally quantified statement since it is asserting something for every prime p.

Since this is a universally quantified statement, to disprove it we need to produce a counterexample. That is, we wish to produce a prime number p_0 such that $2^{p_0} - 1$ is *not* prime. Let us try out some examples in hopes of finding a counterexample.

$$2^2 - 1 = 3, \text{ which is prime.}$$

$$2^3 - 1 = 7, \text{ which is prime.}$$

$$2^5 - 1 = 31, \text{ which is prime.}$$

$$2^7 - 1 = 127, \text{ which is prime.}$$

$$2^{11} - 1 = 2047 = 23 \cdot 89 \text{ is } \textit{not} \text{ a prime.}$$

Thus, we have produced a counterexample.

Disproof. Note that $p = 11$ is prime but $2^p - 1 = 2^{11} - 1 = 2047 = 23 \cdot 89$ is composite, and therefore not prime. This counterexample disproves the given conjecture. □

Discussion 5.31 (Proofs of Existentially Quantified Statements)**.** Consider a existentially quantified statement

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

Methods to prove existence results include

(1) Exhibit $x \in S$ satisfying $P(x)$. This is called a *constructive proof*.

(2) Use other existence theorems (i.e., leverage other results).

(3) Use proof by contradiction. This is *the method of choice for proving existence results*.

Discussion 5.32 (Unique Existence)**.** We want to also mention a variation of the statement above. Recall that the above existentially quantified statement says *there exists an $x \in S$ such that $P(x)$ is true*. We focus on a statement when such an x is unique, that is, not only is $P(x)$ true for this x, x is the only element for which $P(x)$ is true. The statement is then *there exists a unique $x \in S$ such that $P(x)$ is true*, written symbolically as

$$(\exists x \in S,\ P(x)) \wedge (\forall y \in S,\ P(y) \Rightarrow y = x)$$

which is often shortened as

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

So, there are two steps to proving such a statement

Step 1. Existence proof. Prove such an x exists.

Step 2. Uniqueness proof. Prove such an x is unique.

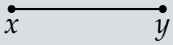
We have already discussed Step 1. For Step 2., one typically does the following

(1) If $x, y \in S$ are such that $P(x)$ and $P(y)$ is true, prove that $y = x$.

(2) If $x, y \in S$ are such that $P(x)$ and $P(y)$ is true and $y \neq x$, then show we obtain a contradiction.

Proposition 5.33. *Let $x, y \in \mathbb{Q}$ such that $x \leqslant y$. There exists a rational number r such that $x \leqslant r \leqslant y$.*

PROOF IDEA. This given proposition is asking us to prove an existentially quantified statement. We aim to give a *constructive* proof, that is, we will explicitly produce a rational number r between x and y. To understand what this rational number could be, it is best to imagine x and y on the number line as follows



What could be a number between these two numbers? A possibility is their midpoint!

Proof. Given rational numbers x and y such that $x \leqslant y$, consider the number

$$r = \frac{x+y}{2}$$

To observe that r is, in fact, a rational number, we may write $x = a/b$ and $y = c/d$ for some integers a, b, c, d where $b, d \neq 0$. Then,

$$r = \frac{x+y}{2} = \frac{a/b + c/d}{2} = \frac{ad+bc}{2bd},$$

and therefore $r \in \mathbb{Q}$, since $ad + bc$, $2bd \in \mathbb{Z}$ with $2bd \neq 0$. Moreover,

$$r - x = \frac{x+y}{2} - x \qquad\qquad y - r = y - \frac{x+y}{2}$$
$$= \frac{x+y-2x}{2} = \frac{y-x}{2} \geqslant 0 \qquad\qquad = \frac{2y-(x+y)}{2} = \frac{y-x}{2} \geqslant 0$$

since $x \leqslant y$. Thus $x \leqslant r \leqslant y$, and hence r is a rational number lying between x and y. □

6. The Contrapositive

Remark 6.1. We will exploit the logical equivalence (Theorem 5.28) to introduce a new method of proof: *Contrapositive*. The theorem says that to prove (or disprove) the implication $P \Rightarrow Q$ is equivalent to proving (or disproving) the implication $\neg Q \Rightarrow \neg P$. Let us spend some time working through examples to understand how one finds the contrapositive of a given implication.

6.1. Finding the Contrapositive

Discussion 6.2 (Steps to Finding the Contrapositive)**.** If one has been provided with a

"if *some statement*, then *some statement*".

one should follow the following steps to determine the contrapositive (in words).

- Identify statements P and Q such that the statement above is $P \Rightarrow Q$.
- Determine $\neg P$ and $\neg Q$. It will be useful to keep Discussion 5.24 in mind.
- Carefully consider the implication $\neg Q \Rightarrow \neg P$, and write it in words.

Example 6.3. We will determine the contrapositive of the given statements.

(a) Consider the statement *if $n = 2$, then n is even.*

- We note that the following statements

$$P : n = 2 \quad \text{and} \quad Q : n \text{ is even}$$

  make it so that the given statement is $P \Rightarrow Q$.
- We now observe that we have

$$\neg P : n \neq 2 \quad \text{and} \quad \neg Q : n \text{ is not even}$$

- The contrapositive is the implication $\neg Q \Rightarrow \neg P$, which is

$$n \text{ is not even} \Rightarrow n \neq 2$$

Therefore the contrapositive of the given statement is *if n is not even, then $n \neq 2$.*

(b) Consider the statement *if I dumped water on you, then you are wet.*

- We note that the following statements

$$P : \text{I dumped water on you} \quad \text{and} \quad Q : \text{you are wet}$$

  make it so that the given statement is $P \Rightarrow Q$.
- We now observe that we have

$$\neg P : \text{I did not dump water on you} \quad \text{and} \quad \neg Q : \text{you are not wet}$$

- The contrapositive is the implication $\neg Q \Rightarrow \neg P$, which is

$$\textit{you are not wet} \Rightarrow \textit{I did not dump water on you}$$

Therefore the contrapositive of the given statement is *if you are not wet, then I did not dump water on you.*

(c) Consider the statement *if* $p \mid ab$, *then* $p \mid a$ *or* $p \mid b$.

- We note that the following statements

$$P : p \mid ab \quad \text{and} \quad Q : p \mid a \text{ or } p \mid b$$

make it so that the given statement is $P \Rightarrow Q$.

- We now observe that we have

$$\neg P : p \nmid ab \quad \text{and} \quad \neg Q : p \nmid a \text{ and } p \nmid b$$

We obtain the latter by using De Morgan's Laws (L7 in Theorem 5.18).

- The contrapositive is the implication $\neg Q \Rightarrow \neg P$, which is

$$p \nmid a \textit{ and } p \nmid b \Rightarrow p \nmid ab$$

Therefore the contrapositive of the given statement is *if* $p \nmid a$ *and* $p \nmid b$, *then* $p \nmid ab$.

6.2. Proofs using Contrapositive

Lecture 18

Discussion 6.4 (Proof by Contrapositive)**.** Recall that a *direct proof* is a way to prove a "$P \Rightarrow Q$" statement, by starting with the hypothesis P and working our way to the conclusion Q. The contrapositive provides us with a new method of proof to prove $P \Rightarrow Q$; it tells us to provide a direct proof of the contrapositive $\neg Q \Rightarrow \neg P$. We start with the negation of the conclusion $\neg Q$ and work our way to the negation of the hypothesis $\neg P$. Here is the general structure of a proof by contrapositive:

Proposition. $P \Rightarrow Q$

Proof. We will prove the contrapositive. Assume *not* Q

an explanation of what not Q *means* (apply definitions and/or other results)

$\vdots$ apply algebra, logic and other techniques

Look, that is what not P *means*

Therefore *not* P.

Since *not* Q implies *not* P, by the contrapositive we have shown that P implies Q. □

Proposition 6.5. *Suppose* $n \in \mathbb{Z}$. *If* n^2 *is odd, then* n *is odd.*

PROOF IDEA. If we were to try and prove this directly, we would begin by applying the definition of being an odd number to n^2, that is, we would write $n^2 = 2a + 1$ for some integer a. It is the unclear what to do next to eventually conclude n is odd.

But we observe that the contrapositive of *if n^2 is odd, then n is odd* is

if n is not odd, then n^2 is not odd

It seems much clearer on how to proceed with this statement!

Proof. Suppose $n \in \mathbb{Z}$. We will prove the contrapositive. Assume that n is not odd, then n is even (by Fact 2.1). By definition, we have $n = 2a$ for some integer k. Therefore

$$n^2 = (2a)^2 = 4a^2 = 2(2a^2)$$

Since k is an integer, so is $2k^2$, and hence by definition n^2 is even. Since $n \in \mathbb{Z}$, this is equivalent to n^2 being not odd.

Since n being not odd implies n^2 is not odd, by the contrapositive we have shown that if n^2 is odd, then n is odd. □

Proposition 6.6. *Suppose $n \in \mathbb{Z}$. Then, n is odd if and only if $3n + 5$ is even.*

PROOF IDEA. Remember that an "if and only if" statement consists of two implications, and therefore we have to prove the proposition in "both directions". Indeed, we will prove this proposition by proving

($\Rightarrow$) If n is odd, then $3n + 5$ is even; and

($\Leftarrow$) If $3n + 5$ is even, then n is odd.

The first of these, the "forward implication", is a problem we may solve using definitions. While for the second of these, the "backward implication", we apply the contrapositive.

Proof. ($\Rightarrow$) Let us prove first that if n is odd then $3n + 5$ is even. Suppose n is an odd integer, then by definition we have $n = 2a + 1$ for some $a \in \mathbb{Z}$. Therefore,

$$\begin{aligned} 3n + 5 &= 3(2a + 1) + 5 \\ &= 6a + 8 \\ &= 2(3a + 4) \end{aligned}$$

Since a is an integer, so is $3a + 4$. Hence, by definition, $3n + 5$ is even.

($\Leftarrow$) Let us now prove that if $3n + 5$ is even, then n is odd. We will prove the contrapositive. Assume n is not an odd integer, and so it is even; then by definition we have $n = 2b$ for some $b \in \mathbb{Z}$. Therefore,

$$\begin{aligned} 3n + 5 &= 3(2b) + 5 \\ &= 6b + 4 + 1 \\ &= 2(3b + 2) + 1 \end{aligned}$$

Since b is an integer, so is $3b + 4$. Hence, by definition, $3n + 5$ is odd, that is, it is not even.

Since n being not odd implies $3n + 5$ is not even, by the contrapositive we have shown that if $3n + 5$ even, then n is odd. □

Proposition 6.7. *Let $a, b \in \mathbb{Z}$, and let p be a prime. If $p \nmid ab$, then $p \nmid a$ and $p \nmid b$.*

PROOF IDEA. One may hope that the proposition is the contrapositive of Lemma 2.30 (ii), and if it were then we would make this observation and direct the reader to the proof of the lemma. However that is not the case! If Lemma 2.30 (ii) is $P \Rightarrow Q$, then our proposition is $\neg P \Rightarrow \neg Q$ which is *not* its contrapositive; the contrapositive being $\neg Q \Rightarrow \neg P$.

We will still use the contrapositive to prove the proposition but we are unable to leverage any previous results.

Proof. Suppose $a, b \in \mathbb{Z}$ and p is a prime. We will prove the contrapositive. Suppose it is not true that $p \nmid a$ and $p \nmid b$, this is equivalent to (using De Morgan's Laws) $p \mid a$ or $p \mid b$. Let us treat these two cases separately

CASE I. Suppose $p \mid a$, then by definition of divisibility, we have $a = pk$ for some integer k. Therefore,

$$ab = (pk)b = p(kb)$$

Since $k, b \in \mathbb{Z}$, so is kb, and hence by definition of divisibility we have $p \mid ab$.

CASE II. Suppose $p \mid b$, then by definition of divisibility, we have $a = p\ell$ for some integer ℓ. Therefore,

$$ab = a(p\ell) = p(a\ell)$$

Since $a, \ell \in \mathbb{Z}$, so is $a\ell$, and hence by definition of divisibility we have $p \mid ab$.

In either case we have concluded that $p \mid ab$, which is equivalent to not being the case that $p \nmid ab$.

Since $p \mid a$ or $p \mid b$ implies $p \mid ab$, by the contrapositive we have shown that if $p \nmid ab$ then $p \nmid a$ and $p \nmid b$. □

Discussion 6.8. Note that in the proof of Proposition 6.7 above, then proofs of the two cases were exactly the same. While in Case I we focused on a, and in Case II we focused on b, and had slightly different variables such as k and ℓ, the mathematical content and characteristic of these two cases is exactly the same. Switching the roles of a and k with b and ℓ is all that we need to move between Cases I and II.

Given a proof involving a case-by-case work, mathematicians have agreed to skip proving additional cases if the proof of these additional cases looks as similar to the first case considered as Case II did compared to Case I. To invoke such an idea, one says **without loss of generality**. It is important to convince yourself by doing scratch work that when you do invoke *without loss of generality*, it is appropriate to do so.

Therefore, if you have two cases like $p \mid a$ and $p \mid b$, and there is essentially no mathematical distinction between the cases, then one is allowed to say *without loss of generality, assume $p \mid a$.* This allows you to skip the $p \mid b$ case entirely.

Proof of Proposition 6.4 Revisited (Condensed). Suppose $a, b \in \mathbb{Z}$ and p is a prime. We will prove the contrapositive. Suppose it is not true that $p \nmid a$ and $p \nmid b$, this is equivalent to (using De Morgan's Laws) $p \mid a$ or $p \mid b$. Without loss of generality, assume $p \mid a$.

By definition of divisibility, we have $a = pk$ for some integer k. Therefore,

$$ab = (pk)b = p(kb)$$

Since $k, b \in \mathbb{Z}$, so is kb, and hence by definition of divisibility we have $p \mid ab$.

Since $p \mid a$ or $p \mid b$ implies $p \mid ab$, by the contrapositive we have shown that if $p \nmid ab$ then $p \nmid a$ and $p \nmid b$. □

7. Contradiction

Lecture 19

Suppose someone stole Priya's wallet at 8 PM last night, they grabbed it from her arms. If Archana is a suspect, but the detective finds conclusive evidence that Archana was across town at 8 PM, then there is now way for her to have grabbed Priya's purse. For mathematical purposes, think about it like this: assume Archana did steal it, then Archana was in two places at once. This is absurd, so she must now have done.

These arguments are called *reductio ad absurdum* – reduction to absurdity. For example, in mathematics one might say "there is not a largest integer, because if there was one and we called it N, then $N+1$ would be a larger integer." One is assuming what ends being false – that there exists a largest integer N, and we are showing that such an assumption would imply something absurd – that N is largest and yet $N+1$ is larger.

This is the main idea behind our next proof technique.

7.1. Contradiction & Examples

Discussion 7.1. Assume R is a statement, and recall that a contradiction $\perp$ is a statement that is always false. Then the logical principal behind **proof by contradiction** is the following logical equivalence

$$R \equiv (\neg R \Rightarrow \perp)$$

R	$\neg R$	$\perp$	$\neg R \Rightarrow \perp$
T	**F**	**F**	**T**
F	**T**	**F**	**F**

If the negation of R gives us a contradiction, that is, if $(\neg R \Rightarrow \perp)$ is true, since the conclusion $\perp$ is always false, the only possibility is for the hypothesis $\neg R$ to be also false. Hence R is true.

Special and Useful Case. If R is of the form of an implication $P \Rightarrow Q$, then to prove $P \Rightarrow Q$ we prove the following

$$\neg(P \Rightarrow Q) \Rightarrow \perp$$

Recall that

$$\neg(P \Rightarrow Q) \equiv \neg(\neg P \vee Q) \equiv P \wedge \neg Q.$$

Thus, to prove $P \Rightarrow Q$, show that

$$(P \wedge \neg Q) \Rightarrow \perp$$

The contradiction we often try to find is $S \wedge \neg S$ for some statement S. In other words, assume P is true and also assume the conclusion Q is false, then we try to find a contradiction $S \wedge \neg S$, finding an appropriate S is the heart of the proof.

Proposition 7.2. *There does not exist a smallest positive rational number.*

PROOF IDEA. This proposition is of the form R, rather than $P \Rightarrow Q$. Therefore to use proof by contradiction, we will assume $\neg R$. That is, let us assume that there *does* exist a smallest

rational number. We will call this smallest rational number $q > 0$, and we may write it as $q = a/b$ for integers a, b where $b \neq 0$. Since $q > 0$, we may assume that $a, b > 0$. How do we find a contradiction? We will find a smaller positive rational number! Therefore we will have simultaneously $S : q$ is the smallest rational number and $\neg S : q$ is not the smallest rational number since we will produce a smaller positive rational number, giving us our contradiction.

Proof. Assume for the sake of contradiction that there is a smallest positive rational number and call this number q. Then, since q is rational,

$$q = \frac{a}{b}$$

for some $a, b \in \mathbb{Z}$. And since $q > 0$, we may assume that $a, b > 0$. Consider the rational number $a/2b > 0$, then

$$\frac{a/2b}{a/b} = \frac{1}{2} < 1$$

Multiplying by $a/b = q > 0$ we obtain

$$0 < \frac{a}{2b} < \frac{a}{b}$$

This contradicts our assumption that q was the smallest positive rational number, and thus there does not exist a smallest positive rational number. □

Discussion 7.3 (Proof by Contradiction)**.** Depending whether our proposition is a statement or an implication we have the following general structure of a proof by contradiction.

Proposition. *R*

Proof. Assume for the sake of contradiction *not R*

an explanation of what not *R means* (apply definitions and/or other results)

⋮ apply algebra, logic and other techniques

Look, that contradicts something we know or have assumed to be true.

Therefore we have arrived at a contradiction. Hence *R*. □

Proposition. $P \Rightarrow Q$

Proof. Assume for the sake of contradiction P and *not R*

an explanation of what P and not *Q means* (apply definitions and/or other results)

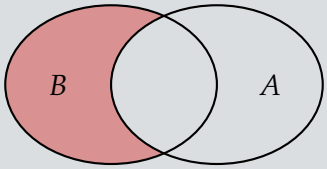
⋮ apply algebra, logic and other techniques

Look, that contradicts something we know or have assumed to be true.

Therefore we have arrived at a contradiction. Hence $P \Rightarrow Q$. □

Proposition 7.4. *If A and B are sets, then* $A \cap (B \setminus A) = \varnothing$.

PROOF IDEA. This proposition makes sense when you look at the Venn diagram



$B \setminus A$

The shaded region is $B \setminus A$, and none of that shaded portion falls inside of the A oval. Since there are no elements inside both A and $B \setminus A$, it makes sense that $A \cap (B \setminus A)$ is the empty set.

But how do we prove it? The conclusion of the proposition is that $A \cap (B \setminus A) = \varnothing$. Since this is saying that something does *not* happen, one may wonder whether a contrapositive proof would work here. Unfortunately the contrapositive says "$A \cap (B \setminus A) \neq \varnothing$, *then* A *or* B *is not a set*", but how would one prove something is not a set? This method of proof does not sound promising.

A proof by contradiction, on the other hand, allows us to assume the hypothesis and the negation of the conclusion, that is, assume A and B are set and $A \cap (B \setminus A) \neq \varnothing$.

Proof. Assume for the sake of contradiction that A and B are sets and $A \cap (B \setminus A) \neq \varnothing$. Then, there exists some $x \in A \cap (B \setminus A)$. By the definition of intersection, this implies $x \in A$ and $x \in B \setminus A$. Now, using the definition of set minus $x \in B \setminus A$ means that $x \in B$ and $x \notin A$. Therefore, we have concluded that $x \in A$ and $x \notin A$, which is absurd and we have obtained our contradiction. Hence $A \cap (B \setminus A) = \varnothing$. □

Proposition 7.5. *Prove that there do not exist integers m and n for which $15m + 35n = 1$.*

PROOF IDEA. Assume for a contradiction that there *are* integers m and n where

$$15m + 35n = 1$$

What can we do now? Even thought we do not know what m and n are, you may in your scratch work plug in values for m and n to get a feel for what is going on. Doing so might help us notice that $15m + 35n$ is always a multiple of 5.

But the right hand side is 1, which is not a multiple of 5. Seems like we are inching towards a contradiction!

Proof. Assume for the sake of contradiction that there does exist integers m and n for which $15m + 35n = 1$. Dividing both sides by 5 we obtain

$$3m + 7n = \frac{1}{5}.$$

Observe that since $m, n \in \mathbb{Z}$, we have that $3m + 7n$ is an integer. But we observe that $1/5$ is not an integer. Therefore we have arrived at a contradiction. Hence there do not exist integers m and n for which $15m + 35n = 1$. □

7.2. Most Famous Proofs in History

Lecture 20

It is time for us to discuss the most famous proof in mathematics – Euclid's proof of the infinitude of primes.

In the following proof, recall that if $n \geqslant 2$ is an integer, then n is either prime or composite – and being composite means you are a product of primes.

Theorem 7.6 (Infinitude of Primes)**.** *There are infinitely many prime numbers.*

Proof. Assume for the sake of contradiction that there are only finitely many primes, say k-many in total. Let $p_1, p_2, \ldots, p_k$ is the complete list of prime numbers, and consider

$$N = p_1 p_2 \cdots p_k + 1$$

We will use N to produce a prime that is not one of those we have assumed to be all the primes. Since $N = p_1 p_2 \cdots p_k + 1 \geqslant 2$, it is either prime or composite.

CASE I. Assume N is prime. Observe that since any prime $\geqslant 2$, we have

$$p_i < p_1 p_2 \cdots p_k < p_1 p_2 \cdots p_k + 1 = N$$

for any $1 \leqslant i \leqslant k$. Therefore if N is prime, and since it is larger than each p_i, it must be a new prime.

CASE II. Assume N is composite. We will first show that no p_i can divide N. Observe that $p_i \mid (p_1 p_2 \cdots p_k)$, and therefore

$$p_1 p_2 \cdots p_k \equiv 0 \bmod p_j$$

We may add 1 to each side, applying Proposition 2.27 (i), to obtain

$$N = p_1 p_2 \cdots p_k + 1 \equiv 1 \bmod p_i$$

We have shown that $N \not\equiv 0 \bmod p_i$, and hence $p_i \nmid N$ for every $1 \leqslant i \leqslant k$.

Since N is composite, it is a product of primes and, in particular, has a prime factor q. But since we have observed that $p_i \nmid N$ for any $1 \leqslant i \leqslant k$, we must have $q \neq p_i$. That is, q is a prime number distinct for those we have assumed to be all the primes.

In both cases we have contradicted the claim that $p_1, p_2, \ldots, p_k$ is an exhaustive list of primes numbers. Therefore there must be infinitely many primes. □

Theorem 7.7 (Irrationality of $\sqrt{2}$)**.** *The number $\sqrt{2}$ is irrational.*

Proof. Assume for the sake of contradiction that $\sqrt{2}$ is rational. Then there must be some non-zero integers a, b such that

$$\sqrt{2} = \frac{a}{b}$$

Moreover, we may assume that this fraction is written in *lowest terms* (or as a *reduced fraction*), meaning that a and b have no common divisors, that is, $\gcd(a, b) = 1$. Then,

$$\sqrt{2} b = a$$

Squaring both sides gives us

$$2b^2 = a^2 \tag{🤚}$$

Since $b^2 \in \mathbb{Z}$, we conclude that $2 \mid a^2$ by definition of divisibility. Therefore by Lemma 2.30 (iii), we conclude that

$$2 \mid a \tag{👉}$$

By definition of divisibility we have $a = 2k$ for some non-zero integer k. Plugging this in (🤚) gives us

$$\begin{aligned} 2b^2 &= (2k)^2 \\ 2b^2 &= 4k^2 \\ b^2 &= 2k^2 && \text{(dividing by 2)} \end{aligned}$$

Hence $2 \mid b^2$, since $k^2 \in \mathbb{Z}$. Thus, using Lemma 2.30 (iii) again, we conclude that

$$2 \mid b \tag{✌}$$

(👉) and (✌) tells us that 2 is a common divisor of a and b. But this contradicts our assumption that a and b had no common divisors. Therefore there $\sqrt{2}$ cannot be rational, meaning it must be irrational. □

8. Functions

Earlier we studied the static properties of sets, which are fundamental to almost everything we do in mathematics. But things get more interesting and dynamic when we start "comparing" sets, functions are what allow us to systematically do this.

8.1. Approaching Functions

Definition 8.1 (Functions)**.** Given a pair of sets A and B. Suppose *every* element of $x \in A$ is associated, in some way, to a unique element of B, which we denote $f(x)$. Then this association is defined to be a **function** f from A to B. This is often denoted as

$$\begin{aligned} f : A &\to B \\ x &\mapsto f(x) \end{aligned}$$

Furthermore,

- A is called the **domain** of f, sometimes denoted as $\text{dom}(f)$.
- B is called the **codomain** of f, sometimes denoted as $\text{codom}(f)$.
- The set $\{f(x) \ : \ x \in A\} \subseteq B$ is called the **range** of f, denoted $\text{range}(f)$.

Discussion 8.2 (Well-defined Functions)**.** When discussing functions, the idea of *unique existence* will show up often (see Discussion 5.32). We have already seen this in the definition of a function above, Definition 8.1.

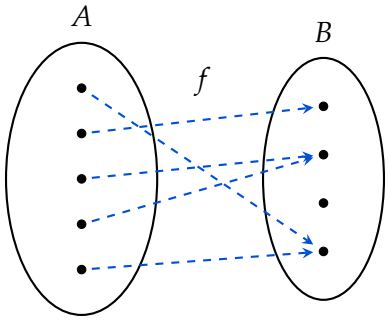
We defined $f : A \to B$ to be a rule which sends *each* $x \in A$ to some $f(x) \in B$. What this means is that $f(x)$ must *exist* (it must be equal to some $b \in B$), and it must be *unique* (it must equal *exactly one* $b \in B$).

This uniqueness property is called the **well-defined**-ness of a function, and may be expressed as follows: for any $a_1, a_2 \in A$

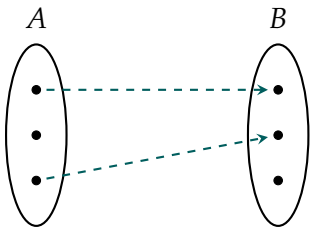
$$\textit{if } a_1 = a_2, \textit{ then } f(a_1) = f(a_2)$$

We will reconcile the above statement with the uniqueness statement as follows: assume the above statement did not hold, then we have $a_1 = a_2$ and $f(a_1) \neq f(a_2)$. This is saying that for a single value of $a = a_1 = a_2$, we have two options $f(a) = f(a_1)$ and $f(a) = f(a_2)$ which are not the same, violating our claim that $f(a)$ must be a unique quantity.

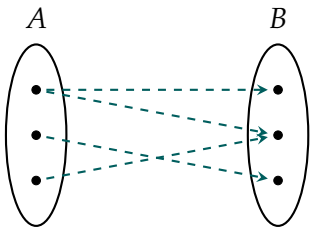
A visual way to depict some function f is given by the following diagram



For a diagram like this to *not* represent a function, it would have to fail either the existence or the uniqueness part of being a function; below are two examples



fails existence



fails uniqueness

Lecture 21

Example 8.3. Consider the following functions

- $f : \mathbb{R} \to \mathbb{Z},\ x \mapsto \lfloor x \rfloor$.
  - ▷ That is, for any $x \in \mathbb{R}$, we have $f(x) = \lfloor x \rfloor$; this is the *floor function*. Given a real number x, the integer $\lfloor x \rfloor$ is the integer you get by rounding down. For example,
  $$\lfloor 3.2 \rfloor = 3 \quad \text{and} \quad \lfloor 7.8 \rfloor = 7.$$
- $g : \{1,2,3,4,5\} \to \{1,4,9,16,25,36,49\},\ t \mapsto t^2$.
  - ▷ That is, for any $t \in \{1,2,3,4,5\}$, we have $g(t) = t^2$.
  - ▷ This is the usual squaring function but you are not allowed to consider the square of any number that is not in the set $\{1,2,3,4,5\}$. For example, $g(-2)$ and $g(6)$ does not make sense, since g can only accept elements as inputs elements from its domain set $\{1,2,3,4,5\}$. The *range* of g is
  $$\{g(t) \ : \ t \in \{1,2,3,4,5\}\} = \{t^2 \ : \ t \in \{1,2,3,4,5\}\} = \{1,4,9,16,25\}$$
- Let $\mathcal{P}_{\text{fin}}(\mathbb{Z})$ is the set of finite subsets of $\mathbb{Z}$ and let $\mathbb{N}_0$ be the set of non-negative integers, and consider the cardinality function
  $$|\cdot| : \mathcal{P}_{\text{fin}}(\mathbb{Z}) \to \mathbb{N}_0,\ X \mapsto |X|$$
  - ▷ For example, $|\{-1,5,12,-3,-27\}| = 5$.
  - ▷ Notice that this function isn't written as most functions are, like $f(x)$ or $g(t)$. The naming of the function is more visually descriptive; the vertical bars go around the input. To make this clearer, we add a little dot between the bars as a placeholder, to show where the element will go: $|\cdot|$.
  - ▷ Matching how we have names the function in this example, we may have named the previous two examples as $\lfloor \cdot \rfloor$ and $(\cdot)^2$ respectively.

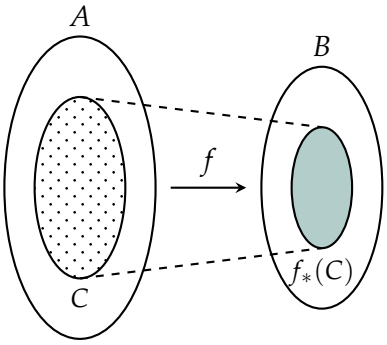
Example 8.4. Here are some abstract examples of functions.

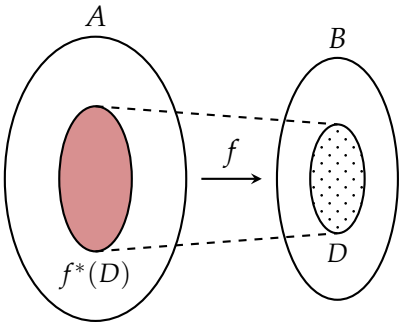
- IDENTITY FUNCTION. For any set X, the *identity function on* X is the function
  $$\begin{aligned} \text{id}_X : X &\to X \\ x &\mapsto x \end{aligned}$$
  That is, this is the function $\text{id}_X(x) = x$.

- INCLUSION FUNCTION. For any non-empty set A, and a subset $S \subseteq A$. The *inclusion function* is the function
$$\begin{aligned} \iota : S &\to A \\ z &\mapsto z \end{aligned}$$
- RESTRICTION FUNCTION. Let $f : A \to B$ be a function, and consider a subset $S \subseteq A$. The *restriction of f to S* is
$$\begin{aligned} f|_S : S &\to B \\ z &\mapsto f(z) \end{aligned}$$
where $\text{dom}(f|_S) = S$. That is, given the rule f on A, we are restricting this rule to the subset S.

Remark 8.5. When can we say two functions are equal? Two functions $f : A \to B$ and $g : C \to D$ are equal if $A = C$, $B = D$ and
$$f(x) = g(x)$$
for every $x \in A = C$.

Definition 8.6 (Images & Preimages)**.** Let $f : A \to B$ be a function, and let $C \subseteq A$ and $D \subseteq B$.

- The **image** of C under f is the set
$$f_*(C) = \{f(x) \ : \ x \in C\} \subseteq B$$


Note that $\text{range}(f) = f_*(A)$.
- The **preimage** (or **inverse image**) of D under f is the set
$$f^*(D) = \{y \in A \ : \ f(y) \in D\} \subseteq A$$


Example 8.7.

- Consider the function $f : \mathbb{R} \to \mathbb{R},\ x \mapsto \pi x - 1$, and consider $\mathbb{Z}_{>0} \subseteq \mathbb{R}$. Then, we have

$$\begin{aligned} f_*(\mathbb{Z}_{>0}) &= \{f(x) \ : \ x \in \mathbb{Z}_{>0}\} \\ &= \{\pi x - 1 \ : \ x \in \mathbb{Z}_{>0}\} = \{\pi - 1, 2\pi - 1, 3\pi - 1, 4\pi - 1, 5\pi - 1, \ldots\} \end{aligned}$$

- Consider the function $f : \mathbb{R} \to \mathbb{Z},\ x \mapsto \lfloor x \rfloor$, and consider $\{2,3\} \subseteq \mathbb{Z}$. Then, we have

$$\begin{aligned} f^*(\{2,3\}) &= \{x \in \mathbb{R} \ : \ f(x) \in \{2,3\}\} \\ &= \{x \in \mathbb{R} \ : \ f(x) = 2 \text{ or } f(x) = 3\} \\ &= \{x \in \mathbb{R} \ : \ f(x) = 2\} \cup \{x \in \mathbb{R} \ : \ f(x) = 3\} \\ &= \{x \in \mathbb{R} \ : \ \lfloor x \rfloor = 2\} \cup \{x \in \mathbb{R} \ : \ \lfloor x \rfloor = 3\} \\ &= \{x \in \mathbb{R} \ : \ 2 \leqslant x < 3\} \cup \{x \in \mathbb{R} \ : \ 3 \leqslant x < 4\} \\ &= \{x \in \mathbb{R} \ : \ 2 \leqslant x < 4\} = [2,4) \end{aligned}$$

8.2. Injections, Surjections and Bijections

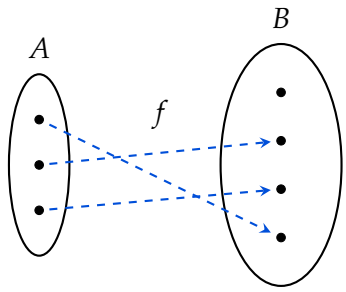
Lecture 22

We will see in this section very important types of functions.

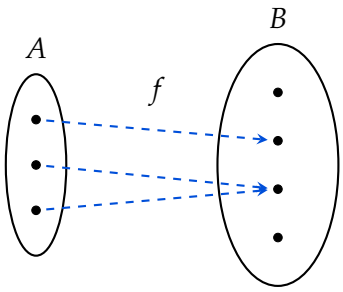
Definition 8.8 (Injective Functions)**.** A function $f : A \to B$ is **injective** (or **one-to-one**) if *for every* $x, y \in A,\ x \neq y$ *implies* $f(x) \neq f(y)$.

That is, if f *maps distinct elements to distinct elements*.

Equivalently, taking the contrapositive, f is **injective** if *for every* $x, y \in A,\ f(x) = f(y)$ *implies* $x = y$. This definition is more convenient for proofs.



an injection from from A to B



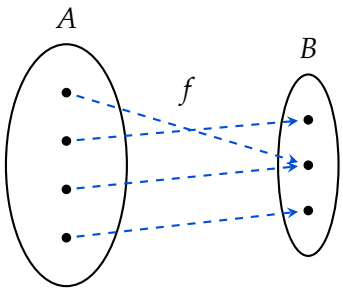
not an injection from A to B

Visually speaking, a function is injective if in the codomain no two arrowheads collide.

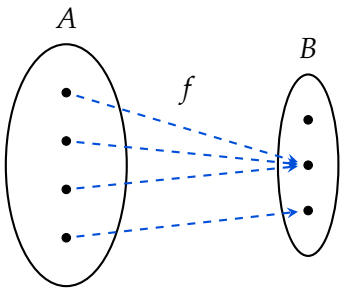
Definition 8.9 (Surjective Functions)**.** A function $f : A \to B$ is **surjective** (or **onto**) if $f(A) = B$.

That is, if *every element of* B *is mapped to by* f. Therefore f is **surjective** if *for every* $b \in B$, *there exists an* $a \in A$ *such that* $f(a) = b$.

Observe that the statement above is equivalent to saying $B \subseteq f(A)$.



a surjection from from A to B



not a surjection from from A to B

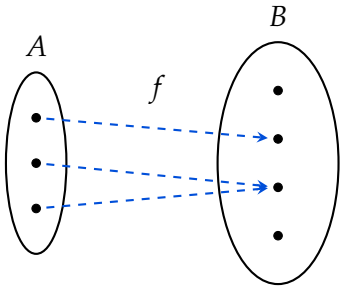
Visually speaking, a function is surjective if every element in the codomain receives an arrow.

Discussion 8.10. When defining a function $f : A \to B$, the ideas of *existence* and *uniqueness* was focused on A – for every $x \in A$, we demand that $f(x)$ exist and be unique.

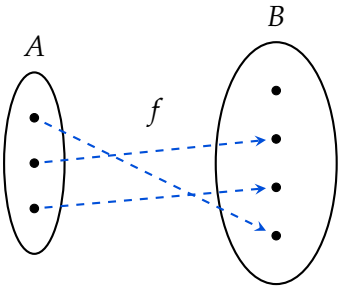
To be injective and surjective, the attention shifts to B. To be surjective means that B has an existence criterion – for every $b \in B$ there *exists* some $a \in A$ that maps to it. And to be injective means that B has a uniqueness-type criterion – for every $b \in B$ there is *at most one* $a \in A$ that maps to it.

Definition 8.11 (Bijective Functions)**.** A function $f : A \to B$ is **bijective** if it is injective and surjective.

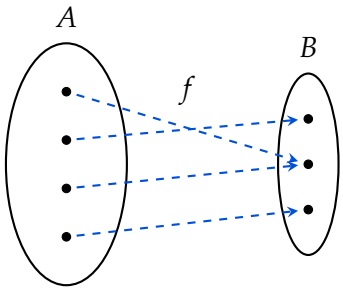
Example 8.12. Let us look at some examples and non-examples.



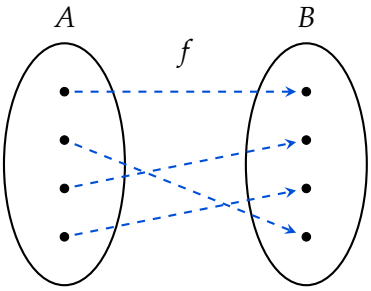
✖ not injective
✖ not surjective
✖ not bijective



✔ is injective
✖ not surjective
✖ not bijective



✖ not injective
✔ is surjective
✖ not bijective



✔ is injective
✔ is surjective
✔ is bijective

Discussion 8.13. As observed previously, defining a function $f : A \to B$ placed the *existence* and *uniqueness* criteria on A. If f is both injective and surjective, then this adds the *existence* and *uniqueness* criteria on B.

Therefore, if f is a bijection, then it has these criteria on both sides: every $a \in A$ is mapped to precisely one $b \in B$, and every $b \in B$ is mapped to by precisely one $a \in A$. In effect, this pairs up each element of A with an element of B. Namely, a is paired with $f(a)$ in this way.

Discussion 8.14 (Proving In/Sur/Bi-jectiveness)**.** Based on definitions, we have the following outline to prove a function is injective.

Proposition. $f : A \to B$ is injective.

Proof. Assume $x, y \in A$ and $f(x) = f(y)$

$\vdots$ apply algebra, logic and other techniques

Therefore $x = y$.

Since $f(x) = f(y)$ implies $x = y$, we conclude that f is injective. □

We have the following outline to prove a function is surjective.

Proposition. $f : A \to B$ is surjective.

Proof. Assume $b \in B$.

$\vdots$ find $a \in A$ such that $f(a) = b$, and show it works

Since every $b \in B$ has an $a \in A$ where $f(a) = b$, we conclude that f is surjective. □

It is important to remember that when you choose $b \in B$, at the start of your surjectivity proof, it must be completely arbitrary. If $B = \mathbb{R}$, make sure you are never assuming that b is positive or negative or nonzero or integer, or anything like that. Your work must be valid regardless of what b is. Recall that this is what we mean when we say that we chose an *arbitrary* $b \in B$.

To prove a function is bijective, we need to prove it is both injective and surjective. Therefore a proof of bijectivity will have both of the proof frameworks presented above.

Example 8.15. Let $\mathbb{R}_+ = \mathbb{R}_{\geqslant 0}$ denote the set of non-negative real numbers. Prove the following.

(a) $f : \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$ is not injective, surjective or bijective.

(b) $g : \mathbb{R}_+ \to \mathbb{R},\ x \mapsto x^2$ is injective, but not surjective or bijective.

(a) $h : \mathbb{R} \to \mathbb{R}_+,\ x \mapsto x^2$ is surjective, but not surjective or bijective.

(a) $k : \mathbb{R}_+ \to \mathbb{R}_+,\ x \mapsto x^2$ is injective, surjective and bijective.

It is worth noting that even though all these functions have the same "rule", they are, in fact, distinct functions since they have either distinct domains or codomains.

PROOF IDEA. Observe that if we wish to prove f is *not injective*, we need to produce a pair $x, y \in \mathbb{R}$ such that $x \neq y$ but $x^2 = f(x) = f(y) = y^2$.

While to prove g is not surjective, we need to produce a $y \in \mathbb{R}$ such that for no $x \in \mathbb{R}_+$ we have $y = f(x) = x^2$.

Proof.

(a) Observe that $f(-2) = 4 = f(2)$ but $2 \neq -2$, showing that f is not injective. Also observe that $f(x) = x^2 \geqslant 0$ for all $x \in \mathbb{R}$, showing that there does exist an $x \in \mathbb{R}$ such that $f(x) = -1$. Since -1 is in the codomain of f, this proves that f is not surjective. Since f is neither injective nor surjective, it is also not bijective. □

(b) Similar to (a), since $g(x) = x^2 \geqslant 0$ for all $x \in \mathbb{R}$, showing that there does exist an $x \in \mathbb{R}$ such that $g(x) = -1$. Since -1 is in the codomain of f, this proves that g is not surjective. This also proves that g is not bijective.

To see that g is injective, assume $x, y \in \mathbb{R}_+$ such that $g(x) = g(y)$. Then,

$$\begin{aligned} x^2 &= y^2 \\ x^2 - y^2 &= 0 \\ (x-y)(x+y) &= 0 \end{aligned}$$

Therefore either $x - y = 0$ or $x + y = 0$. If $x - y = 0$, then we have $x = y$, as we wished to prove. Now, assume $x + y = 0$, then $y = -x$. But, since $x, y \in \mathbb{R}_+$, necessarily we must have $x = y = 0$. Hence, even in this case, we have $x = y$.

Thus, we have shown that $g(x) = g(y)$ implies $x = y$, and therefore g is injective. □

(c) Observe that h is not injective, just like in (a), since $h(-2) = 4 = h(2)$ but $2 \neq -2$. This also proves that h is also not bijective.

To see that h is surjective, consider some $b \in \mathbb{R}_+$. Since $b \geqslant 0$, the positive square root exists, and let $x = \sqrt{b} \in \mathbb{R}_+$. Then, we have

$$h(x) = x^2 = (\sqrt{b})^2 = b$$

Therefore we have shown that for every $b \in \mathbb{R}_+$ there exists an $x \in \mathbb{R}_+$ such that $h(x) = b$. Hence h is surjective. □

(d) The fact that k is injective follows the same exact reasoning as with g in (b), and the fact that k is surjective follows the same exact reasoning as with h in (c). Since k is both injective and surjective, we have proven that k is bijective. □

Lecture 23

Example 8.16. The function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ where $f(x, y) = (x + 2y, 2x + 3y)$ is a bijection.

SCRATCH WORK. To prove the function is bijective, we wish to prove it is injective and surjective. The scratch work for injective is essentially the proof, so let us focus on surjectivity.

To show that the function is surjective, we must show that for an arbitrary $(a,b) \in \mathbb{Z} \times \mathbb{Z}$, there exists some $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ such that $f(x,y) = (a,b)$. How do we find such an (x,y)? Scratch work! We want

$$\begin{aligned}(a,b) &= f(x,y)\\ (a,b) &= (x+2y, 2x+3y)\end{aligned}$$

When are two ordered pairs equal? Certainly $(2,3) \neq (4,5)$, but also $(2,3) \neq (2,5)$ and $(2,3) \neq (4,3)$. In order to have two ordered pairs equal, *both* their coordinates must be equal! Thus, in order to have $(a,b) = (x+2y, 2x+3y)$, we must have

$$x + 2y = a \quad \text{and} \quad 2x + 3y = b$$

We wish to figure out which x and y make this work; so we do algebra to solve for x and y.

Given equations

$$\begin{aligned}x + 2y &= a\\ 2x + 3y &= b\end{aligned}$$

Multiplying the first equation by 2, we obtain

$$\begin{aligned}2x + 4y &= 2a\\ 2x + 3y &= b\end{aligned}$$

Subtracting the second equation from the first, we obtain $y = 2a - b$. Substituting this y in $x + 2y = a$, get us

$$\begin{aligned}x &= a - 2y\\ &= a - 2(2a - b) = -3a + 2b\end{aligned}$$

According to this scratch work, in order for $f(x,y) = (a,b)$, we would need

$$(x,y) = (-3a + 2b, 2a - b).$$

We will use this in the surjective half our proof below.

Proof. We will prove that f is injective and surjective.

INJECTIVITY. Assume $f(x_1,y_1) = f(x_2,y_2)$ for any $(x_1,y_1), (x_2,y_2) \in \mathbb{Z} \times \mathbb{Z}$. Notice that

$$\begin{aligned}f(x_1,y_1) &= f(x_2,y_2)\\ (x_1 + 2y_1, 2x_1 + 3y_1) &= (x_2 + 2y_2, 2x_2 + 3y_2)\end{aligned}$$

We therefore have

$$\begin{aligned}x_1 + 2y_1 &= x_2 + 2y_2 \qquad (✂)\\ 2x_1 + 3y_1 &= 2x_2 + 3y_2\end{aligned}$$

Multiplying (✂) by 2 gives us

$$\begin{aligned}2x_1 + 4y_1 &= 2x_2 + 4y_2\\ 2x_1 + 3y_1 &= 2x_2 + 3y_2\end{aligned}$$

Subtracting the bottom from the top leaves

$$y_1 = y_2 \qquad (❦)$$

We plug y_2 in for y_1, by (❀), into (✂)

$$x_1 + 2y_2 = x_2 + 2y_2$$

Subtracting the $2y_2$ from both sides, we see that

$$x_1 = x_2$$

Combined with (❀), we may conclude that $(x_1, y_1) = (x_2, y_2)$.

We have shown that $f(x_1, y_1) = f(x_2, y_2)$ implies $(x_1, y_1) = (x_2, y_2)$, proving that f is injective.

SURJECTIVITY. Consider any $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. We wish to find a $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ such that $f(x, y) = (a, b)$. We claim that $(x, y) = (-3a + 2b, 2a - b)$ works. First, note that since $a, b \in \mathbb{Z}$, we have $-3a + 2b, 2a - b \in \mathbb{Z}$, and therefore $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.

Second, observe that

$$\begin{aligned} f(x, y) &= f(-3a + 2b, 2a - b) \\ &= ((-3a + 2b) + 2(2a - b), 2(-3a + 2b) + 3(2a - b)) \\ &= (-3a + 2b + 4a - 2b, -6a + 4b + 6a - 3b) \\ &= (a, b) \end{aligned}$$

Therefore we have shown that for any (a, b) from the codomain, there exists some (x, y) from the domain such that $f(x, y) = (a, b)$. Hence f is surjective.

Since f is both injective and surjective, it is a bijection. □

8.3. The Composition

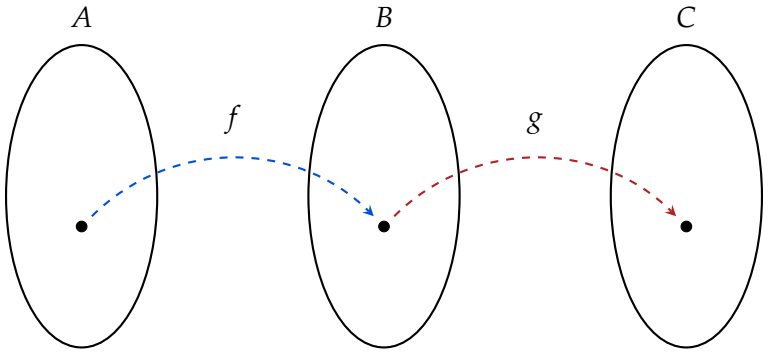
Definition 8.17 (Composition of Functions)**.** 5 Let $f : A \to B$ and $g : B \to C$ be functions. Then their **composition** is the function

$$g \circ f : A \to C$$

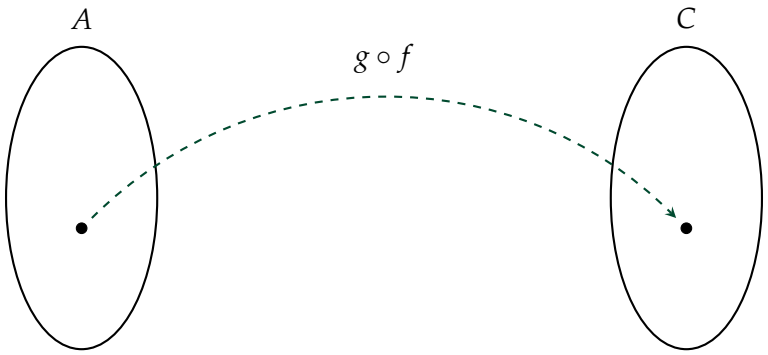
where, for any $a \in A$,

$$(g \circ f)(a) = g(f(a))$$

Visually one may consider



which can be combined to produce



In particular, $\text{dom}(g \circ f) = \text{dom}(f)$ and $\text{codom}(g \circ f) = \text{codom}(g)$.

Example 8.18. Recall that $\mathbb{R}_+$ is the set of non-negative reals, and $\mathbb{N}_0$ the set of non-negative integers. Remember that the $g \circ f$ is a function from the *domain of* f to the *codomain of* g.

- Suppose

$$f : \mathbb{R} \to \mathbb{R}, \text{ where } f(x) = x + 1 \qquad g : \mathbb{R} \to \mathbb{R}_+, \text{ where } g(x) = x^2$$

  Then, $g \circ f : \mathbb{R} \to \mathbb{R}_+$ where

$$(g \circ f)(x) = g(f(x)) = g(x+1) = (x+1)^2$$

- Suppose

$$f : \mathbb{R} \to \mathbb{R}_+, \text{ where } f(x) = x^2 \qquad g : \mathbb{R}_+ \to \mathbb{R}_+, \text{ where } g(x) = x + 1$$

  Then, $g \circ f : \mathbb{R} \to \mathbb{R}_+$ where

$$(g \circ f)(x) = g(f(x)) = g(x^2) = x^2 + 1$$

- Recall that the *floor function* is the rounding-down-function, e.g. $\lfloor 13.721 \rfloor = 13$.

$$f : \mathbb{R} \to \mathbb{Z}, \text{ where } f(x) = \lfloor x \rfloor \qquad g : \mathbb{Z} \to \mathbb{N}_0, \text{ where } g(x) = |x|$$

  Then, $g \circ f : \mathbb{R} \to \mathbb{N}_0$ where

$$(g \circ f)(x) = g(f(x)) = g(\lfloor x \rfloor) = |\lfloor x \rfloor|$$

  For instance, $f(-7.29) = -8$ and $g(-8) = 8$, implying that $(g \circ f)(-7.29) = 8$.

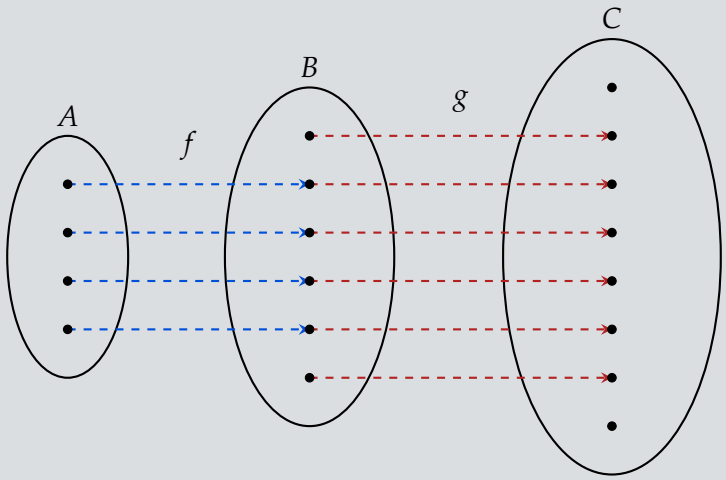
Lecture 24

Proposition 8.19. *Let $f : A \to B$ and $g : B \to C$ be functions.*

(1) If both f and g are injective, then their composition $g \circ f$ is also injective.

(2) If both f and g are surjective, then their composition $g \circ f$ is also surjective.

PROOF IDEA.

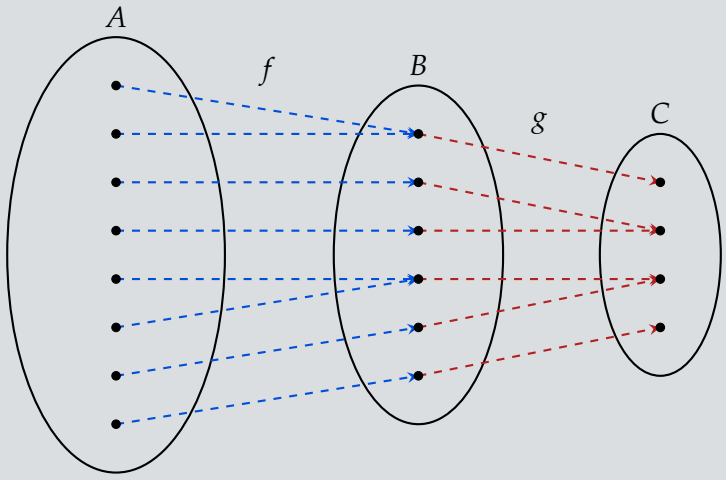


Proof of (1). Suppose f and g are injective, we need to show $g \circ f$ is injective. Consider any $x, y \in A$ such that $(g \circ f)(x) = (g \circ f)(y)$, we need to show $x = y$. We have

$$\begin{aligned} g(f(x)) &= g(f(y)) \\ f(x) &= f(y) && \text{since } g \text{ is injective} \\ x &= y && \text{since } f \text{ is injective} \end{aligned}$$

Since $g(f(x)) = g(f(y))$ implies $x = y$, hence $g \circ f$ is injective. □

PROOF IDEA.



Proof of (2). Suppose f and g are surjective, we need to show $g \circ f$ is surjective. We aim to show that for every $c \in C$, we can find an $a \in A$ such that $(g \circ f)(a) = c$.

Consider any $c \in C$, since g is surjective, there exists a $b \in B$ such that $g(b) = c$. Since f is surjective, for this b, there exists an $a \in A$ such that $f(a) = b$. Hence,

$$(g \circ f)(a) = g(f(a)) = g(b) = c.$$

Thus $g \circ f$ is surjective. □

8.4. Invertibility

Recall from Example 8.4 the notion of the identity function.

Definition 8.20 (Inverse of a Function)**.** The **inverse** of a function $f : A \to B$ is a function $g : B \to A$ such that

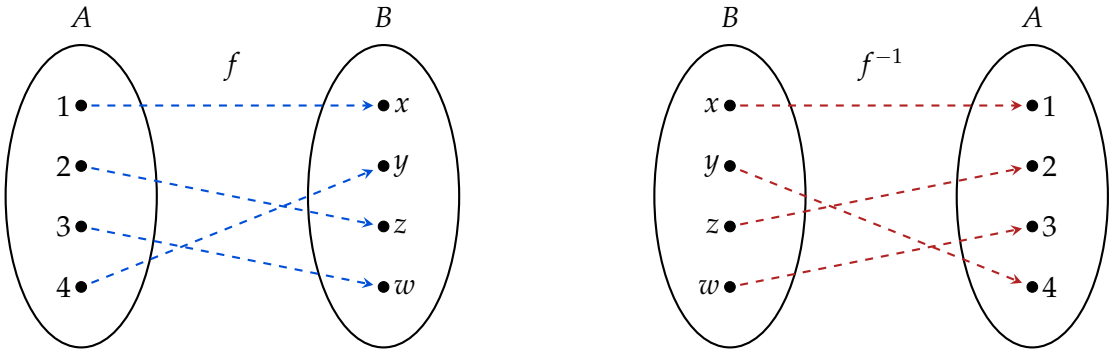
$$g \circ f = \mathrm{id}_A \quad \text{and} \quad f \circ g = \mathrm{id}_B$$

That is, for any $a \in A$ and $b \in B$, we have

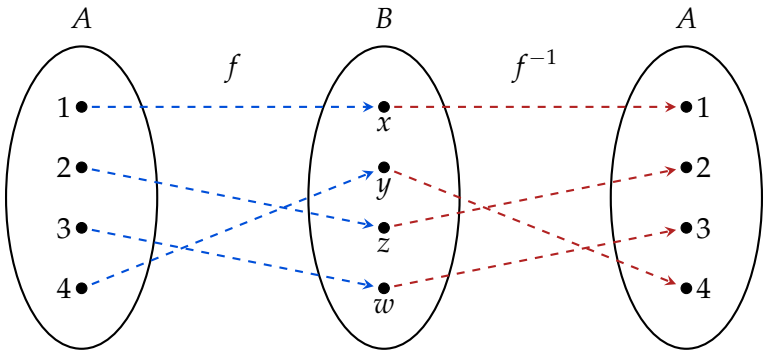
$$g(f(a)) = a \quad \text{and} \quad f(g(b)) = b$$

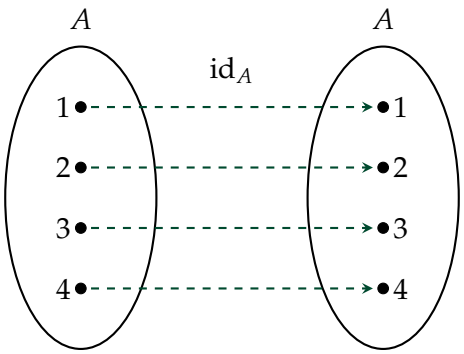
If it exists, g is unique and denoted as f^{-1}.

Discussion 8.21. An inverse undoes the function. If x was sent to y by f (that is, $f(x) = y$), then y will be sent to x by f^{-1} (that is, $f^{-1}(y) = x$). For example

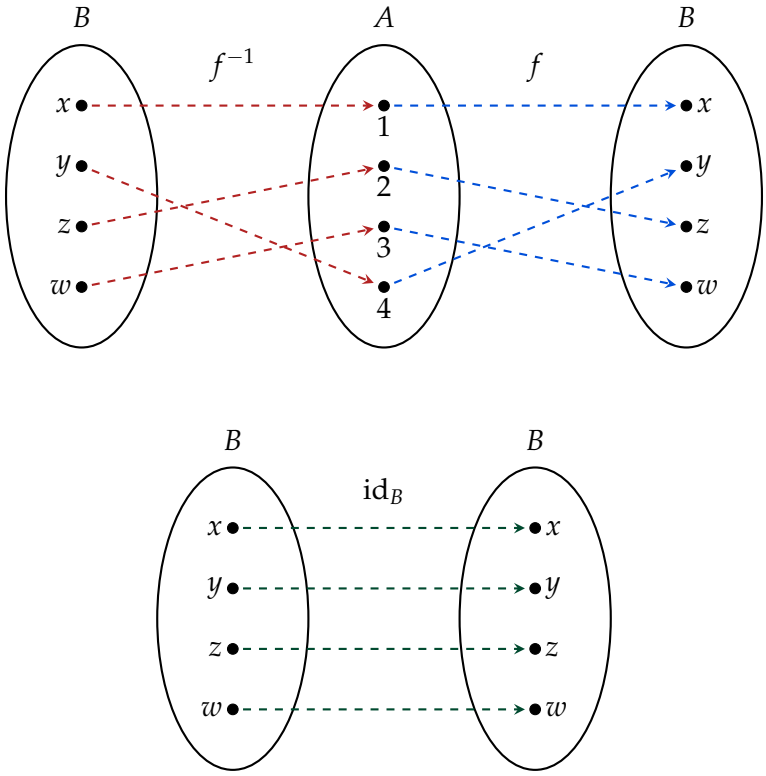


Combined, we get the identity function. Here is $f^{-1} \circ f = \mathrm{id}_A$





Here is $f \circ f^{-1} = \mathrm{id}_B$



Example 8.22. Here are some more examples of functions with inverses.

- Consider the function $f : \mathbb{R} \to \mathbb{R},\ x \mapsto x + 1$, then $f^{-1} : \mathbb{R} \to \mathbb{R}$ is the function $f^{-1}(x) = x - 1$. To see this, note that

$$\begin{aligned}(f \circ f^{-1})(x) = f(f^{-1}(x)) &= f(x-1) \\ &= (x-1)+1 = x = \mathrm{id}_{\mathbb{R}}(x)\end{aligned}$$

  showing that $f \circ f^{-1} = \mathrm{id}_{\mathbb{R}}$. Likewise,

$$\begin{aligned}(f^{-1} \circ f)(x) = f^{-1}(f(x)) &= f^{-1}(x+1) \\ &= (x+1)-1 = x = \mathrm{id}_{\mathbb{R}}(x)\end{aligned}$$

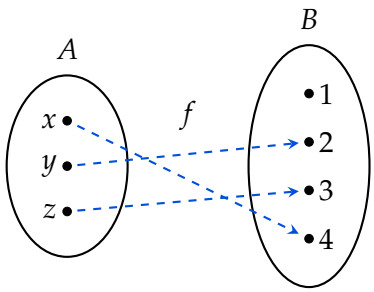
  showing that $f^{-1} \circ f = \mathrm{id}_{\mathbb{R}}$.

- If $f : \mathbb{R}_+ \to \mathbb{R}_+$ where $f(x) = x^2$, then $f^{-1} : \mathbb{R}_+ \to \mathbb{R}_+$ is the function $f^{-1}(x) = \sqrt{x}$.

- If $f : [0,1] \to [0,2]$ where $f(x) = 2x$, then $f^{-1} : [0,2] \to [0,1]$ is the function $f(x) = \dfrac{1}{2}x$.

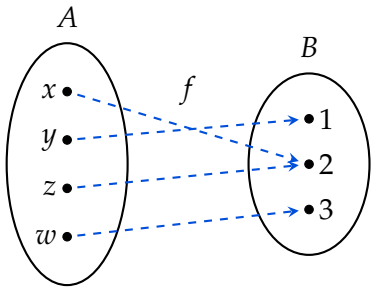
Discussion 8.23. Consider the function $f : \{1,2,3,4\} \to \{x,y,z,w\}$ in Discussion 8.21, it had an inverse and was a bijection. This was no accident. In fact, *only* bijections have inverses. The reason for this can be seen in two parts.

- *f must be surjective.* Suppose f were not a surjection, e.g.



  Why does this function not have in inverse? If it did, where would it take 1?

- *f must be injective.* Suppose f were not a injection, e.g., then



  Why does this function not have in inverse? If it did, where would it take 2?

Theorem 8.24. *A function $f : A \to B$ is invertible if and only if f is a bijection.*

Proof. ($\Rightarrow$) Assume $f : A \to B$ is invertible, that is, there exists $f^{-1} : B \to A$. We will prove that f is both an injection and a surjection, thereby showing that f is a bijection.

Let us first show that f is surjective. Consider any $b \in B$, and define $a = f^{-1}(b) \in A$. Then, we observe that

$$f(a) = f(f^{-1}(b)) = \mathrm{id}_B(b) = b$$

Therefore f is surjective.

Let us now show that f is injective. Consider any pair $a_1, a_2 \in A$ such that $f(a_1) = f(a_2)$, then

$$\begin{aligned} f(a_1) &= f(a_2) \\ f^{-1}(f(a_1)) &= f^{-1}(f(a_2)) && \text{(apply } f^{-1} \text{ on both sides)} \\ \mathrm{id}_A(a_1) &= \mathrm{id}_A(a_2) \\ a_1 &= a_2 \end{aligned}$$

Therefore f injective.

Since f is both injective and surjective, it is bijective.

($\Leftarrow$) Assume f is bijective. To show f is invertible, we wish to define its inverse.

For a $b \in B$, we define $g(b) = a$ if and only if $f(a) = b$. We claim that g is a function and $g = f^{-1}$.

To show g is a function, we wish to show that $g(b)$ is defined for every $b \in B$ and $g(b)$ is unique for every $b \in B$.

EXISTENCE. Consider any $b \in B$, since f is surjective, there exists an $a \in A$ such that $f(a) = b$. Therefore, we have $g(b) = a$, for any $b \in B$.

UNIQUENESS/WELL-DEFINED. Consider $b_1, b_2 \in B$ such that $b_1 = b_2$, we wish to show that $g(b_1) = g(b_2)$. Let $a_1 = g(b)$ and $a_2 = g(b)$. Since $a_1 = g(b_1)$ and $a_2 = g(b_2)$, one has $f(a_1) = b_1$ and $f(a_2) = b_2$. Therefore $f(a_1) = b_1 = b_2 = f(a_2)$, and since f is injective, we conclude $a_1 = a_2$.

Thus g is a well-defined function.

We now wish to show that $g = f^{-1}$, i.e., we want to show that

$$g \circ f = \mathrm{id}_A \quad \text{and} \quad f \circ g = \mathrm{id}_B$$

For any $a \in A$, let $b = f(a)$. By definition, we have $g(b) = a$. Therefore, we get

$$g(f(a)) = a \quad \text{and} \quad f(g(b)) = b$$

Hence, we have proven that $g = f^{-1}$. Thus we have that f is invertible. □

Example 8.25. The function $f : \mathbb{R} \setminus \{2\} \to \mathbb{R} \setminus \{3\}$, where $f(x) = 3 + \dfrac{6}{x-2}$, is a bijection.

PROOF IDEA. With Theorem 8.24 in mind, we will show f is bijective by producing an inverse of f. We do some algebra to obtain the inverse function.

Step 1. First let $y = f(x)$, that is,

$$y = 3 + \frac{6}{x-2}$$

Step 2. Switch x with y. That is,

$$x = 3 + \frac{6}{y-2}$$

Step 3. Solve for y.

$$3 + \frac{6}{y-2} = x$$

$$\frac{6}{y-2} = x - 3 \qquad \text{subtracting 3}$$

$$\frac{y-2}{6} = \frac{1}{x-3} \qquad \text{taking reciprocal, we can since } b \neq 3$$

$$y - 2 = \frac{6}{x-3} \qquad \text{multiplying by 6}$$

$$y = 2 + \frac{6}{x-3} \qquad \text{adding 2}$$

Note that this expression is $\neq 2$.

Step 4. The resulting y is your candidate for an inverse function.

Proof. Define $g : \mathbb{R} \setminus \{3\} \to \mathbb{R} \setminus \{2\}$ as

$$g(x) = 2 + \frac{6}{x-3}$$

Then,

$$\begin{aligned}
(g \circ f)(x) = g(f(x)) &= 2 + \frac{6}{f(x)-3} & (f \circ g)(x) = f(g(x)) &= 3 + \frac{6}{g(x)-2} \\
&= 2 + \frac{6}{\left(3 + \frac{6}{x-2}\right) - 3} & &= 3 + \frac{6}{\left(2 + \frac{6}{x-3}\right) - 2} \\
&= 2 + \frac{6}{\left(\frac{6}{x-2}\right)} & &= 3 + \frac{6}{\left(\frac{6}{x-3}\right)} \\
&= 2 + \frac{6(x-2)}{6} & &= 3 + \frac{6(x-3)}{6} \\
&= 2 + (x-2) & &= 3 + (x-3) \\
&= x & &= x
\end{aligned}$$

Hence $f \circ g = \mathrm{id}$ and $g \circ f = \mathrm{id}$. Thus, f is invertible and, by Theorem 8.24, f is bijective. □

9. Relations

9.1. Equivalence Relations

Lecture 25

Discussion 9.1. In Section 2.5 we studied modular arithmetic. For example, one has

$$-2 \equiv 3 \bmod 5 \qquad 3 \equiv 3 \bmod 5 \qquad 8 \equiv 3 \bmod 5 \qquad 13 \equiv 3 \bmod 5$$

Since all these numbers are congruent to 3 modulo 5, there is a sense of "equivalence" between these numbers and 3. Perhaps this is emphasised by the fact that we may swap these numbers over $\equiv$, i.e., we also have

$$3 \equiv -2 \bmod 5 \qquad 3 \equiv 3 \bmod 5 \qquad 3 \equiv 8 \bmod 5 \qquad 3 \equiv 13 \bmod 5$$

Moreover, not only are, for example, -2 and 13 congruent to 3 modulo 5, they are, in fact, congruent to each other modulo 5. That is, one has

$$13 \equiv -2 \bmod 5 \qquad -2 \equiv 8 \bmod 5 \qquad 8 \equiv 13 \bmod 5$$

One can check this by nothing that $(13-(-2))$, $(-2-8)$, $(8-13)$ are numbers divisible by 5.

Therefore, in this mod-5 world, every element in the set $\{-2, 3, 8, 13\}$ is equivalent to each other and itself. Furthermore, this extends! In the following five sets, elements of a given set will be congruent to each other and themselves modulo 5

- $\{\ldots, -10, -5, 0, 5, 10, 15, 20, 25, \ldots\}$
- $\{\ldots, -9, -4, 1, 6, 11, 16, 21, 26, \ldots\}$
- $\{\ldots, -8, -3, 2, 7, 12, 17, 22, 27, \ldots\}$
- $\{\ldots, -7, -2, 3, 8, 13, 18, 23, 28, \ldots\}$
- $\{\ldots, -6, -1, 4, 9, 14, 19, 24, 29, \ldots\}$

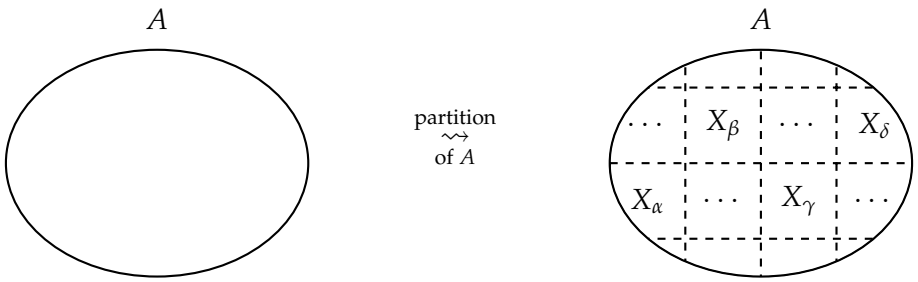
These five sets are called *equivalence classes* of mod-5 *equivalence relation*. They further have the important property that they *partition* the set $\mathbb{Z}$, i.e., every integer is in exactly one of these sets.

Definition 9.2 (Partitions)**.** A **partition** of a set A is a collection of non-empty subsets of A such that any element of A is in one, and only one, of these subsets.

Formally speaking, a collection $\mathcal{S} = \{X_\alpha\}_{\alpha \in I}$ of subsets of A, where $X_\alpha \neq \varnothing$ for every $\alpha \in I$, is called a **partition** of A if

(1) $X_\alpha \cap X_\beta = \varnothing$ if $\alpha \neq \beta$ (we say X_α and X_β are **(mutually) disjoint**)

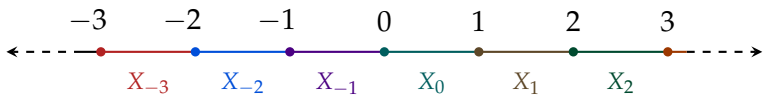
(2) $\bigcup_{\alpha \in I} X_\alpha = A$.



Example 9.3.

(1) One can partition $\mathbb{Z}$ into the sets of even and odd integers. That is, the sets $E = \{2k : k \in \mathbb{Z}\}$ and $O = \{2k+1 : k \in \mathbb{Z}\}$, then one has $E \cap O = \varnothing$ and $E \cup O = \mathbb{Z}$. Therefore $\{E, O\}$ is a partition of $\mathbb{Z}$.

(2) For $\mathbb{R}$ the set of real numbers, we will produce a partition of $\mathbb{R}$. For any integer m, consider the subset $X_m = [m, m+1) = \{x \in \mathbb{R} : m \leqslant x < m+1\}$ of $\mathbb{R}$.



Observe that

$$\begin{cases} X_m \cap X_k = \varnothing, \text{ for any pair of integers } m \neq k; \text{ and} \\ \mathbb{R} = \bigcup_{m \in \mathbb{Z}} X_m \end{cases}$$

Thus, $\{X_m : m \in \mathbb{Z}\}$ is a partition of $\mathbb{R}$.

(3) The five sets produced at the end of Discussion 9.1

- $\{\ldots, -10, -5, 0, 5, 10, 15, 20, 25, \ldots\}$
- $\{\ldots, -9, -4, 1, 6, 11, 16, 21, 26, \ldots\}$
- $\{\ldots, -8, -3, 2, 7, 12, 17, 22, 27, \ldots\}$
- $\{\ldots, -7, -2, 3, 8, 13, 18, 23, 28, \ldots\}$
- $\{\ldots, -6, -1, 4, 9, 14, 19, 24, 29, \ldots\}$

also partition $\mathbb{Z}$.

Discussion 9.4. We may ask several questions here: what properties are required to give us this partition property? Is it important that 5 is a prime? Will this work, say, if we switched from 5 to 6? Even better, can one describe the properties that produce a partition without any mention of modular arithmetic?

We will momentarily use the following notation: write $a \sim_5 b$ if $a \equiv b \bmod 5$. With this, the reader should attempt prove the following properties

(ER) $a \sim_5 a$ for all $a \in \mathbb{Z}$.

(ES) If $a \sim_5 b$, then $b \sim_5 a$, for all $a, b \in \mathbb{Z}$.

(ET) If $a \sim_5 b$ and $b \sim_5 c$, then $a \sim_5 c$, for all $a, b, c \in \mathbb{Z}$.

Not only does mod-5 property satisfy these three important properties, it turns out these three are *precisely* what is required to product the partition/equivalence property.

What we mean by this: assume we only had a set A, and for some pairs of elements from A, and one is told that a is *"related"* to b (denoted $a \sim b$) while for other apirs one is told that a is *"not related"* to b (denoted $a \not\sim b$). But you are told nothing else about A and you have no idea what rule is determining

which pairs are related and which are not.

Given that setup, here's the miracle: if $\sim$ satisfies the three properties we observed above, then set "naturally" partitions itself into *equivalence classes*. If $\sim$ does not satisfy one or more of these three properties, then set will not partition itself into "equivalence classes", i.e., at least one element will either be in no class or will be in multiple. For example,

Example 9.5. Suppose $A = \mathbb{Z}$ and we say that $a \sim b$ if $a \geqslant b$. One may notice that $a \sim a$, since $a \geqslant a$ for all $a \in \mathbb{Z}$ (property (ER)). One may also notice that if $a \sim b$ and $b \sim c$ then $a \sim c$, since $a \geqslant b$ and $b \geqslant c$, we have $a \geqslant c$ (property (ET)). But if $a \sim b$, we have $b \not\sim a$, since if $3 \geqslant 2$ but $2 \not\geqslant b$, so it fails the (ES) property.

Let us now consider the "equivalence classes"; consider for 6, all the numbers $a \in \mathbb{Z}$ such that $a \sim 6$, which is the set

$$\{6, 7, 8, 9, \ldots\}$$

What about the set of all numbers for which $4 \sim a$? Or $8 \sim a$? These are the sets

$$\{4, 5, 6, 7, \ldots\} \quad \text{and} \quad \{8, 9, 10, 11, \ldots\}$$

But observe that these sets are not mutually disjoint, and thus will not partition $\mathbb{Z}$!

Definition 9.6. A **relation** on a set A is any *ordered* relationship between pairs of elements of A for which the pair is either *related* or is *not related* (but never both). If $a, b \in A$, we denote $a \sim b$ if a is related to b, and $a \not\sim b$ if a is not related to b.

If $\sim$ is a relation and $a \in A$, we define the **right class** generated by a to be the set

$$\{r \in A \ : \ a \sim r\}$$

and define the **left class** generated by a to be the set

$$\{s \in A \ : \ s \sim a\}$$

Definition 9.7. An **equivalence relation** on a set A is a relation with the following three properties

- (Reflexive) $a \sim a$ for all $a \in A$.
- (Symmetric) if $a \sim b$, then $b \sim a$, for all $a, b \in A$.
- (Transitive) if $a \sim b$ and $b \sim c$, then $a \sim c$, for all $a, b, c \in A$.

Given an equivalence relation $\sim$ and $a \in A$, the left and right classes generated by a are equal and we refer to this set

$$[a] = \{x \in A \ : \ x \sim a\}$$

as the **equivalence class** of a.

Example 9.8. Recall the *floor function* is the function that rounds down. For example, $\lfloor 2.6 \rfloor = 2$. Now, let $\sim$ be the relation on $\mathbb{R}$ where

$$a \sim b \quad \text{if} \quad \lfloor a \rfloor = \lfloor b \rfloor$$

Let us verify that this is an equivalence relation

- (Reflexive) For any $a \in \mathbb{R}$, we certainly have $\lfloor a \rfloor = \lfloor a \rfloor$.
- (Symmetric) If $\lfloor a \rfloor = \lfloor b \rfloor$, then we surely have $\lfloor b \rfloor = \lfloor a \rfloor$, for any $a, b \in \mathbb{R}$.
- (Transitive) If $\lfloor a \rfloor = \lfloor b \rfloor$ and $\lfloor b \rfloor = \lfloor c \rfloor$, then we surely have $\lfloor a \rfloor = \lfloor c \rfloor$, for any $a, b, c \in \mathbb{R}$.

How about the equivalence class of a real number under this equivalence relation? Let us consider

$$\begin{aligned}[3] = \{x \in \mathbb{R} \,:\, x \sim 3\} &= \{x \in \mathbb{R} \,:\, \lfloor x \rfloor = \lfloor 3 \rfloor = 3\} \\ &= \{x \in \mathbb{R} \,:\, 3 \leqslant x < 4\} \\ &= [3, 4)\end{aligned}$$

Let us also consider

$$\begin{aligned}[13.7] = \{x \in \mathbb{R} \,:\, x \sim 13.7\} &= \{x \in \mathbb{R} \,:\, \lfloor x \rfloor = \lfloor 13.7 \rfloor = 13\} \\ &= \{x \in \mathbb{R} \,:\, 13 \leqslant x < 14\} \\ &= [13, 14)\end{aligned}$$

While we have yet to prove that equivalence classes produce a partition of our set (Theorem 9.12), indeed that is the case, and the partition this equivalence relation produces is Example 9.3 (2).

Example 9.9.

- Let $\sim$ be the relation on $\mathbb{Z}$ where

  $$a \sim b \quad \text{if} \quad a \equiv b \bmod n$$

  is an equivalence relation, where the resulting partition is governed by remainders left when divided by n.
- Let $\sim$ be the relation on $\mathscr{T}$, the set of all triangles, where

  $$\triangle_1 \sim \triangle_2 \quad \text{if} \quad \triangle_1 \text{ is similar to } \triangle_2$$

  is an equivalence relation.

Example 9.10. Let $\sim$ be the relation on $\mathbb{R}^2 \setminus \{(0,0)\}$ where

$$(x, y) \sim (u, v) \quad \text{if} \quad \text{there exists a } \lambda \in \mathbb{R} \setminus \{0\} \text{ such that } (x, y) = (\lambda u, \lambda v)$$

Let us verify that this is an equivalence relation

- (Reflexive) For any $(x, y) \in \mathbb{R}^2 \setminus \{(0,0)\}$, we may take $\lambda = 1$ and then $(x, y) = (\lambda x, \lambda y)$. Therefore $(x, y) \sim (x, y)$.
- (Symmetric) If $(x, y) \sim (u, v)$, then there exists a $\lambda \in \mathbb{R} \setminus \{0\}$ such that $(x, y) = (\lambda u, \lambda v)$. Then, observe that $(u, v) = (x/\lambda, y/\lambda)$ since $\lambda \neq 0$. Therefore $(u, v) \sim (x, y)$.
- (Transitive) If $(x, y) \sim (u, v)$ and $(u, v) \sim (a, b)$, then there exist $\lambda, \mu \in \mathbb{R} \setminus \{0\}$ such that $(x, y) = (\lambda u, \lambda v)$ and $(u, v) = (\mu a, \mu b)$. Therefore $(x, y) = (\lambda\mu a, \lambda\mu b)$, where $\lambda\mu \in \mathbb{R} \setminus \{0\}$, and hence $(x, y) \sim (a, b)$.

How about the equivalence classes under this relation? Let us consider

$$\begin{aligned}[(3,5)] &= \{(x,y) \in \mathbb{R}^2 \ : \ (3,5) \sim (x,y)\} \\ &= \{(x,y) \in \mathbb{R}^2 \ : \ (x,y) = (3\lambda, 5\lambda), \ \text{ for some } \lambda \in \mathbb{R} \setminus \{0\}\} \\ &= \{(x,y) \in \mathbb{R}^2 \ : \ x = 3\lambda \ \text{ and } \ y = 5\lambda, \ \text{ for some } \lambda \in \mathbb{R} \setminus \{0\}\} \\ &= \{(3\lambda, 5\lambda) \in \mathbb{R}^2 \ : \ \lambda \in \mathbb{R} \setminus \{0\}\}\end{aligned}$$

This is nothing but the line defined by the equation $3y = 5x$, minus the origin. Let us also consider

$$\begin{aligned}[(1,0)] &= \{(x,y) \in \mathbb{R}^2 \ : \ (1,0) \sim (x,y)\} \\ &= \{(x,y) \in \mathbb{R}^2 \ : \ (x,y) = (\lambda, 0), \ \text{ for some } \lambda \in \mathbb{R} \setminus \{0\}\} \\ &= \{(x,y) \in \mathbb{R}^2 \ : \ x = \lambda \ \text{ and } \ y = 0, \ \text{ for some } \lambda \in \mathbb{R} \setminus \{0\}\} \\ &= \{(\lambda, 0) \in \mathbb{R}^2 \ : \ \lambda \in \mathbb{R} \setminus \{0\}\}\end{aligned}$$

This is nothing but the line defined by the equation $y = 0$, minus the origin.

Example 9.11. For $A = \{\text{all people}\}$, let $\sim$ be a relation on A where

$$P_1 \sim P_2 \quad \text{if and only if} \quad \text{age}(P_1) = \text{age}(P_2)$$

This is an equivalence relation. Here is my equivalence class

$$\begin{aligned}[\text{Deewang}] &= \{P \in A \ : \ P \sim \text{Deewang}\} \\ &= \{P \in A \ : \ \text{age}(P) = \text{age}(\text{Deewang}) = 28\} \\ &= \{\text{all people that are 29 years of age}\}\end{aligned}$$

Age is certainly a way to partition the set of all people.

Theorem 9.12. *Assume $\sim$ is an equivalence relation on A. Then the set of equivalence classes under $\sim$, denoted $A/\sim$, is a partition of A.*

Before we prove this theorem, let us prove a useful lemma.

Lemma 9.13. *Suppose $\sim$ is an equivalence relation on a set A, and let $a, b \in A$. Then,*

$$[a] = [b] \quad \textit{if and only if} \quad a \sim b$$

Proof. ($\Rightarrow$) Assume $[a] = [b]$. Since $\sim$ is an equivalence relation, $a \sim a$, and therefore $a \in [a]$. Since $[a] = [b]$, by assumption, we deduce that $a \in [b]$. Hence, by definition, $a \sim b$.

($\Leftarrow$) Assume $a \sim b$. Since we wish to prove that $[a] = [b]$, we must show that $[a] \subseteq [b]$ and $[b] \subseteq [a]$.

Let us prove $[a] \subseteq [b]$. Consider $x \in [a]$, then by definition $x \sim a$. Since $a \sim b$ and since $\sim$ is an equivalence relation, by the transitive property we conclude that $x \sim b$. Therefore, by definition, $x \in [b]$. Hence $[a] \subseteq [b]$.

Let us prove $[b] \subseteq [a]$. Consider $y \in [b]$, then by definition $y \sim b$. Since $a \sim b$ and since $\sim$ is an equivalence relation, by symmetry we have $b \sim a$. Therefore, we have $y \sim b$ and $b \sim a$, by the transitive property we conclude that $y \sim a$. Therefore, by definition, $y \in [a]$. Hence $[b] \subseteq [a]$.

Since $[a] \subseteq [b]$ and $[b] \subseteq [a]$, we have proven that $[a] = [b]$. □

Proof of Theorem 9.12. □

Proposition 9.14. *Let $\mathcal{S} = \{X_\alpha\}_{\alpha \in I}$ be a partition of a set A. Then, there exists an equivalence relation $\sim$ on A such that the resulting partition by equivalence classes is the given partition $\mathcal{S}$.*

Sketch of Proof.

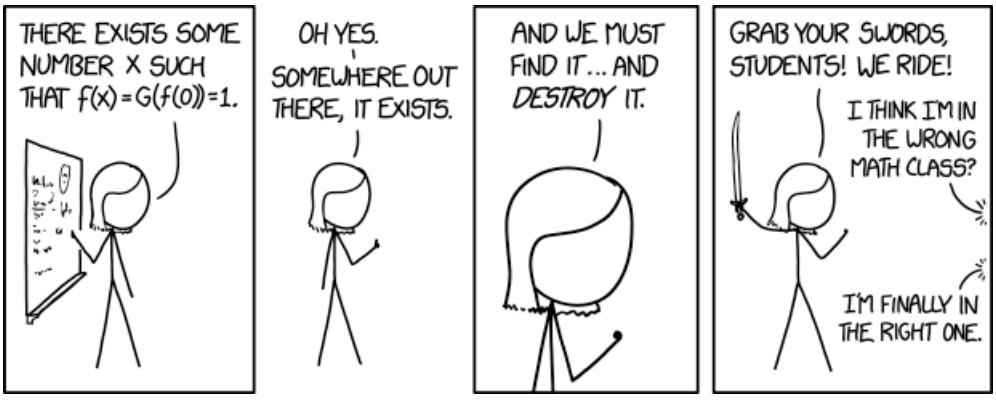
References

[CPZ18] G. Chartrand, A.D. Polimeni, and P. Zhang, *Mathematical Proofs: A Transition to Advanced Mathematics*, Pearson, 2018.

[Cum21] J. Cummings, *Proofs: A Long-form Mathematics Textbook*, The Long-Form Math Textbook Series, CreateSpace Independent Publishing Platform, 2021.

Solving a problem for which you know there's an answer is like climbing a mountain with a guide, along a trail someone else has laid. In mathematics, the truth is somewhere out there in a place no one knows, beyond all the beaten paths. And it's not always at the top of the mountain. It might be in a crack on the smoothest cliff or somewhere deep in the valley.

– Yoko Ogawa, *The Housekeeper and the Professor*



EXISTENCE PROOF (by xkcd)