MATH 101

Professor: Sebastien Vasey

Notes by Michele Tienni
Lowell House
Cambridge, MA 02138
micheletienni@college.harvard.edu

Please note that these notes are not official and they are not to be considered as a substitute for your notes. Specifically, you should not cite these notes in any of the work submitted for the class (problem sets, exams). The author does not guarantee the accuracy of the content of this document. If you find a typo (which will probably happen) feel free to email me.

Contents

Date: December 3, 2018.

1. Friday, September 7

1.1. **Preliminaries.** This course is an introduction to proof-based mathematics. All the texts for the class (indicated on the course website) are freely available online, and there will be recommended readings for each class. There will be two homework assignments a week (excluding midterms and vacations), for a total of 20. There is no requirement for this class.

The four topics of this class are

(i) proofs,
(ii) set theory,
(iii) group theory,
(iv) analysis/topology.

Broadly,

(i) proofs are going to be the foundation of this class and are going to be our main tool;
(ii) set theory is a broad topic, but some of the results we will be concerned with concern *sizes of infinity*. While this may sound confusing, it has a precise formulation. It tells us (among other things) that the "size" of the natural numbers is less than that of the real numbers (which we write $|\mathbb{N}| < |\mathbb{R}|$);
(iii) group theory is the study of objects like the Rubik cube, i.e. objects on which one can performs certain types of transformations. These transformations need to be reversible, and the order matters. The first time you will see the definition of a group you may not realize how the Rubik cube is an example, but it will become clearer as we delve more into the subejct;
(iv) analysis is the study of functions, sequences, and more generally the *real line* (i.e. the real numbers seen as a line) and its subsets.

1.2. **Proofs.** There are some differences between math and other branches of science. For example, in contrast with disciplines such as physics, it is not enough to show that something works in some suitable cases to convince someone that what we are saying is true. Instead, we require very clear, unambiguous explanations of *why* something is true. This is what a proof is for. There are several ways to learn what a proof is. One is to just do a lot of proofs (and we will do this throughout the semester). But it is also useful to find out what a proof is by answering the question: *what is not a proof*?

The sheet you have been handed today provides an example of a flawed proof. It has several positive aspects: it is pretty, it is (too) simple, and it has plenty of pictures (which can be useful to illustrate what is going on). On the other hand, we see that without pictures it would be very hard to figure out what it says. In fact, the phrasing is very ambiguous. For example, what does it mean to *remove corners*? It could mean a lot of things, but this is not specified in the text. In a way, it is specified in the pictures, but in this case the pictures are misleading. In fact, the tricky part is that here the pictures are not only used to illustrate, but also to *explain*. The most controversial step in this "proof" is certainly the one where the process is carried out to infinity. Infinity is a very tricy object; even in an analysis class, it takes a whole course to learn what it means to take something "to infinity." In this case, however, the hard step is not emphasized at all. In correct proofs, the hardest steps are the ones we spend most time on, and that's *because* they are the hardest steps.

Student question: This looks similar to the limit of a Riemann sum. Why does it not work?
Answer: There are many differences. For example, in this case we are talking about a length. At any rate, the mathematical problem in the proof is not quite the reason why we are discussing it. In fact, it is hard to discuss the mathematical content of this "proof" precisely because it is not clear. We might say that the mathematical flaw in this proof is that it claims that a certain limit commutes with integration, which is not the case. But this is beyond the scope of the discusison.

In the end, we have seen that even if a proof is wrong it can still have educational value: in this case, analyzing a wrong proof made us think about what a proof should be like.
It is now time to start exploring simple proofs. We are going to start by proving that the sum of two even integers is even. For example, $2+6=8$, an even number. Similarly, $4+6=10$, again an even number. You might think this is completely obvious, but we still should have a proof, just in case a skeptic comes around and does not believe you. Let us now work out a proof for the following statement:

Theorem 1.1. *The sum of two even integers is even.*

A proof should rely on *common ground* shared with your *target audience*. In this case, the target audience is a student of this class–potentially a very skeptical one! In this case, we can assume that the target audience shares the knowledge of the terms in the following definition:

Definition 1.2. An integer x is **even** if x can be expressed as the product of 2 and an integer, i.e. $x = 2a$ for some integer a.

We see that the first part of the definition is in simple English, while in the latter part (the one after "i.e.") we reformulate it using mathematical symbols. Also note that we usually emphasize the term to be defined.

Student question: Are the two parts of the definition equivalent, and is one preferrable to the other when writing a proof?
Answer: Yes, although sometimes you might prefer the one with more mathematical symbols for clarity.

Student question: Why are we justified in proving things this way (e.g. talking about integers this way)?
Answer: Another necessary component of a proof is that everyone agrees with its underlying logic. We usually use our judgement to establish whether or not this is the case. In this case, for example, we can safely assume that the logic is clear.

Now we have defined our terms with words whose meaning everyone agrees on, and we can start our proof:

Proof. Take two arbitrary even integers x and y. By definition, $x = 2a$ and $y = 2b$ for some integers a and b. Therefore

$$x + y = 2a + 2b = 2(a + b)$$

and so $x+y = 2c$ where $c = a+b$ is also an integers. Therefore $x+y$ is even by definition. $\square$

2. Monday, September 10

2.1. **Proof strategies.**

We will start by introducing some terminology.

A **definition** is an unambiguous explanation of a word or phrase. For example:

Definition 2.1. An integer x is **even** if $x = 2a$ for some integer a.

Definition 2.2. An integer x is **odd** if $x = 2b + 1$ for some integer b.

A **theorem** is a statement that has been proved to be true. For example,

Theorem 2.3. *The sum of two even integers is even.*

Theorem 2.4. *The series*

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots = \sum_{n=1}^{\infty} \frac{1}{n}$$

diverges

Theorem 2.5. *Any differentiable function is continuous.*

Theorem 2.6. *The area of a circle of radius r is πr^2.*

There are synonims of theorems, namely **corollary**, **lemma**, and **proposition**. These have a slightly different use than **theorem**, but the mathematical meaning is the same–they are statements that have been proven to be true.

A **proof** is a written verification that a theorem is true. There are several kind of proofs.

2.1.1. *Direct proof.*

We use this kind of proof to prove something of the form

If P, then Q.

We call P the **hypothesis**, and Q the **conclusion**. An example of the above is the statement

If x and y are even, then $x + y$ is even.

In this case, P is the sentence "x and y are even," and Q is "$x + y$ is even."

We shall now see how to prove such a statement by using a direct proof.

Theorem 2.7. *If x and y are even, then $x + y$ is even.*

Proof.

A direct proof always starts by assuming the hypothesis. We therefore start as follows:

Assume x and y are even.

At this point, we expand the definitions involved in the statement.

Since x is even, $x = 2a$ for some integer a (by definition of even). Similarly, $y = 2b$ for some integer b.

The reason why we are expanding the definition is that we want to go from P to Q. Since we already know the end goal of this proof (namely, concluding that Q) it is always a good idea to expand while keeping in mind Q. In particular, we can look at Q and reverse-engineer the process by compressing back to the definitions, as follows:

Thus $x + y = 2a + 2b = 2(a + b)$. This means that $x + y = 2c$, where $c = a + b$ is an integer, and therefore $x + y$ is even by definition.

□

Student question: In the above proof, do we not have to prove that c is also an integer?

Answer: The fact that the sum of two integers is an integer is one of the basic facts we ca always assume in a proof. If we really wanted to be careful we would want to start from the very axiom of the integers and work from there.

Student question: Is an axiom a theorem?

Answer: I haven't talked about axioms yet, but an **axiom** is something which is *assumed* to be true.

The statement "if P then Q" is *not the same* as "if Q then P." For example, we know that if $1 = 2$, then $0 = 0$ (this is the basic logical fact that anything follows from a contradiction). However, swapping hypothesis and conclusion yields that if $0 = 0$, then $1 = 2$, which is false. Similarly, we can consider our theorem and swap P and Q to get that if $x + y$ is even, then x and y are even, which is false (they could be both odd).

Another proof strategy is **proof by cases**.

2.1.2. *Proof by cases.* Consider the theorem

Theorem 2.8. *If n is a natural number, then*

$$1 + (-1)^n(2n - 1)$$

is a multiple of 4.

Let's see what happens if we attempt a direct proof.

Direct proof. Assume n is a natural number. . . . Thus

$$1 + (-1)^n(2n - 1) = 4k$$

for some integer k. Therefore $1 + (-1)^n(2n - 1)$ is a multiple of 4. □

What could we do in the middle? As a part of our draft work, we might start by listing some cases:

- for $n = 0$: $1 + 2 \cdot 0 - 1 = 0$;
- for $n = 1$: $1 + (-1) \cdot (2 \cdot 1 - 1) = 0$;
- for $n = 2$: $1 + 1 \cdot (2 \cdot 2 - 1)$.

We see that a pattern emerges that has to do with whether or not n is even. We can then divide the proof in two cases, the one where n is even and the one where it is odd.

What could we do in the middle? As a part of our draft work, we might start by listing some cases:

Direct proof. Assume n is a natural number.

Case 1: n is even.

...

Thus

$$1 + (-1)^n(2n - 1) = 4k$$

for some integer k. Therefore $1 + (-1)^n(2n - 1)$ is a multiple of 4.

Case 2: n is odd.

...

Thus

$$1 + (-1)^n(2n - 1) = 4k$$

for some integer k. Therefore $1 + (-1)^n(2n - 1)$ is a multiple of 4.

□

What goes in the blanks now? A crucial fact is to prove that $(-1)^n$ is 1 when n is even and -1 when n is odd. To prove this, we see that

$$(-1)^{2a} = \left((-1)^2\right)a = 1^a = 1$$

and

$$(-1)^{2b+1} = (-1)\left((-1)^2\right)^b = -1.$$

We are now ready to complete the proof.

Direct proof. Assume n is a natural number.

Case 1: n is even.

If n is even, then $n = 2a$ for some integer a. Then

$$(-1)^n = \left((-1)^2\right)^a = 1^a = 1$$

and therefore

$$1 + (-1)^n\,(2n - 1) = 1 + (2 \cdot (2a) - 1) = 4a.$$

Thus

$$1 + (-1)^n(2n - 1) = 4k$$

for some integer k. Therefore $1 + (-1)^n(2n - 1)$ is a multiple of 4.

Case 2: n is odd.

We can write $n = 2b + 1$ for some integer b. Then

$$1 + (-1)^n (2n - 1) = 1 - (2 \cdot (2b + 1) - 1) = 4b.$$

Thus

$$1 + (-1)^n (2n - 1) = 4k$$

for some integer k. Therefore $1 + (-1)^n (2n - 1)$ is a multiple of 4.

□

A third strategy is a **proof by contrapositive**.

2.1.3. *Proof by contrapositive.* We saw earlier that the statement "if P, then Q" is not the same as "if Q, then P." However, "if P, then Q" is equivalent to "if not Q, then not P." The latter form is called the **contrapositive** of the original statement. We also write "not Q" as "$\sim Q$" and we denote implication by a bold right arrow, as in "$\sim Q \Rightarrow \sim P$."

For an example of a proof by contrapositive, consider the following example:

Theorem 2.9. *If xy is odd, then both x and y are odd.*

If we attempted to use a direct proof, we would soon find out that it does not work. This is a sign that we might benefit from using the contrapositive. Such a proof would look as follows:

Proof by contrapositive. The first step is to negate Q, and assume its negation:

Assume that at least one of x or y is even.

Student question: Does this mean that they could both be even?

Answer: Yes. The original form of Q can be reformlated as

Q: x is odd *and* y is odd.

Therefore its negation is

$\sim Q$: (not x is odd) *or* (not y is odd),

that is to say, x is even or y is even. It is important to note that in math we are more precise than when speaking everyday English; in particular, in math "or" is *always* inclusive (meaning that both sides can be true), whereas this might not be true in some English sentences. A good resource to learn more about logical negation in math is Chapter 2 of the text by Hammack.

Student question: In a contrapositive proof can one also use the strategy of proof by cases?

Answer: Yes. Contrapositive proof is usually only the first step, and one usually proceed by direct proof or proof by cases.

Going back to our proof, we note that we just assumed $\sim Q$. At this point, it looks like we should use cases, and consider separately the cases when only one is even and when both are.

Case 1. x is even. In this case, $x = 2a$ and therefore $xy = 2ay = 2c$ where $c = ay$ is an integer. Therefore xy is even.

Now we note that any other case is very similar to this one, and we can say this in the next step.

Case 2. y is even. Completely similar to case 1.

The above is an example of invoking no loss of generality. This is a piece of mathematical jargon, and as a rule one should use it only when no doubt arises.

□

The last strategy we are going to discuss is **proof by contradiction**.

2.1.4. *Proof by contradiction.* In this case, to prove P we assume $\sim P$ and derive somtething false. By doing so, we show that $\sim P$ cannot be true and therefore P must be true. For example:

Definition 2.10. A real number is **rational** if

$$x = \frac{a}{b}$$

where a and b are integersand $b \neq 0$.

Theorem 2.11. *$\sqrt{2}$ is not rational.*

To prove this by direct proof would be very hard, since we cannot check all rational numbers. Therefore, we prove this by contradiction.

Proof. Suppose $\sqrt{2}$ is rational. Then $\sqrt{2} = a/b$ for some integers a, b with $b \neq 0$. We assume that we chose a, b such that they have no common divisor, i.e. the fraction is reduced. By squaring both sides,

$$2 = a^2/b^2$$

and therefore $2b^2 = a^2$. We are now going to show that both of them are even, which mean that a/b was not reduced in the first place. We know for sure that a^2 is even (by definition). Therefore a is even (left as an exercise–if the square of an integer is even then the integer itself is even). This means that $a = 2k$ for some integer k, and therefore

$$2b^2 = a^2 = 4k^2,$$

which means that $b^2 = 2k^2$. By the same argument as above, b is even, which leads to a contradiction. □

This was a bit fast, so it is recommended that you go over it on your own.

3. Friday, September 14

3.1. **More on proofs.** The last thing we did last time was proving that $\sqrt{2}$ is irrational. This is the hardest theorem we've seen so far. Legend has it that when Pythagoras discovered this fact he kept it secret since it clashed with Pythagorean beliefs.

We will now see another example of a proof by contradiction.

Theorem 3.1. *There are infinitely many prime numbers.*

Definition 3.2. An integer x **divides** an integer y if $y = ax$ for some integer a. We also say that y is a **multiple** of x.

Definition 3.3. A natural number n is **prime** if $n \geq 2$ and the only positive divisors of n are 1 and n.

Example 3.4. Example of prime numbers are 2, 3, 5, 7, 11, 13, and so on.

Does the above list continue forever? The answer is yes (Theorem 3.1).

Proof of Theorem 3.1. Assume for a contradiction that there are only finitely many primes. We list all of them as $p_1, p_2, \dots, p_n$. Consider now the number

$$a = p_1 p_2 \cdots p_n + 1.$$

a has at least one prime divisor q. In fact, either a is prime, in which case $q = a$, or it is not prime, in which case it has another divisor d such that $1 < d < a$. So $a = d \cdot b$ for some integer b, and $1 < b < a$. We can now repeat the above step with d, b in place of a until you reach a prime divisor.

(We are waving our hands a little bit here because we really need a proof technique that we have not seen yet, but the idea is that this procedure always works because each step yields a number which is smaller than the original; we will prove this more rigorously this time.)

Since q dividese a, $a = qb$ for some integer b. So

$$p_1 p_2 \cdots p_n + 1 = a = qb,$$

and since q is prime, $q = p_k$ for some k. So

$$p_1 \cdots p_n + 1 = p_k b.$$

Since p_k is a factor in $p_1 \cdots p_{k-1} p_k p_{k+1} \cdots p_n$, we can divide both sides of the above equation by p_k to get

$$p_1 \cdots p_{k-1} p_{k+1} \cdots p_n + \frac{1}{p_k} = b.$$

After subtracting $p_1 \cdots p_{k-1} p_{k+1} \cdots p_n$ from both sides, we get that

$$\frac{1}{p_k} = b - p_1 \cdots p_{k-1} p_{k+1} \cdots p_n.$$

However, the right hand side is an integer (since it is obtained by subtracting two integers), while the left hand side is not, since $p_k > 1$. This is a contradiction.

□

3.2. **If and only if.** We saw that a statement of the form

If P, then Q

is *not* the same as

If Q, then P.

The latter is called the **converse** of the former. If both $P \Rightarrow Q$ and $Q \rightarrow P$ are true, we say

P **if and only if** Q,

which is also written "$P \Leftrightarrow Q$" or "P iff Q."

Example 3.5.

Theorem 3.6. *x is an odd integer if and only if x^2 is an odd integer.*

Proof. First we prove that if x is odd then x^2 is odd.

Assume x is odd. Then $x = 2a + 1$ for some integer a. Then

$$\begin{aligned} x^2 =& (2a+1)^2 \\ =& 4a^2 + 4a + 1 \\ =& 2c + 1 \end{aligned}$$

for some c.

Second, we prove that if x^2 is odd then x is odd.

We prove the contrapositive, namely that if x is even then x^2 is even.

Assume x is even. Then $x = 2b$ for some integer b. Thus

$$\begin{aligned} x^2 =& 4b^2 \\ =& 2(2b^2) \end{aligned}$$

and so x^2 is even. □

3.3. **For all/There exists.** Another way to write

If x and y are even then $x + y$ is even

is

For all even integers x and y, $x + y$ is even.

Another example of such a statement is

For all irrationals x and y, $x + y$ is irrational.

This is a false statement. Sometimes in math we are asked to disprove false statement. But how do we prove that something isn't true? It means proving the negation of the statement. In other words, to disprove a statement P we have to prove not P.

What is

not (for all x $R(x)$)?

There are many ways to write down such a negation, but one of these is

There exists x not $R(x)$.

For example,

not for all leaves x x is green

is the same as

there exists a leaf x x is not green,

i.e. there is a nongreen leaf. Therefore to disprove

for all irrationals x and y, $x + y$ is irrational

we must prove

there exists irrationals x and y such that $x + y$ is rational.

Bonus question: what is

not there exists x $R(x)$?

The answer is

for no x, $R(x)$,

i.e.

for all x not $R(x)$.

To prove a statement of the form "there exists ...," one thing we can do is finding an example.

Example 3.7.

Theorem 3.8. *There is an even prime number n*

Proof. Take $n = 2$. □

Example 3.9.

Theorem 3.10. *For all real numbers x, there exists a real number y such that $x < y$.*

How do we write this statement in the form "if P, then Q?" One way is

If x is a real number, then there exists a real number y such that $x < y$.

Now that we have the statement in this form, we can prove it using a direct proof.

Proof. Assume x is a real number. Take $y = x + 1$. Then $x < x + 1 = y$. □

WARNING: A statement of the form "for all x there exists y ..." is *not* the same as "there exists y such that for all x ...."

Example 3.11. Consider the statement

There exists a real number y such that for all x, $x < y$.

This is obtained from Theorem 3.10 by using the procedure you have been warned about. It is a false statement, and it is directly disproved by Theorem 3.10 itself.

Example 3.12. To say that "for every door, there is a key that opens it" is not the same as saying that "there is a key that opens every door."

Consider now the following theorem:

Theorem 3.13. *There exists irrational numbers x and y such that x^y is rational.*

We are now going to give a non-constructive proof, i.e. a proof that does not involve finding an example.

Proof. Consider the number $\sqrt{2}^{\sqrt{2}}$. Either it is rational or it is irrational.

Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational. Take $x = \sqrt{2}$ and $y = \sqrt{2}$.

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational. Take $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. Then

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^{2} = 2$$

which is rational.

In both cases we found x and y such that x^y is irrational. □

4. Monday, September 17

4.1. **Mathematical induction.** Mathematical induction is a very important example of a proof technique. The word "induction" is used by philosopher in a different way, but in math it denotes a very rigorous method of proving something. Last time we proved that there are infinitely many primes. At some point in the proof we claimed that every natural number $n \geq 2$ has a prime divisor. This was a sub-claim of the proof, but it was not an obvious one and we kind of swept it under the rug. The idea of the proof was that if n is prime then we are done, and if not we can write n as $n = ab$ for integers a, b with $1 < a < n$ and $1 < b < n$. If a is prime, we are done. If not, we can write it as the product of two smaller numbers, and keep going. Intuitively, any time we use arguments that rely on phrases like "keep going" and "and so on," we can use induction to make the proof precise. Let's see induction at work.

Theorem 4.1. *Any natural number is either even or odd.*

(As a note, there is a debate as to whether natural numbers include 0. In this class we will define natural number to omit 0, and use the term **non-negative integers** otherwise.)

There are several ways to prove this, but it is not so easy to prove it directly. The idea of the proof is as follows: 1 is odd, 2 is even, 3 is odd, . . . and so on. In general, if n is even, then $n+1$ is odd, and if n is odd, then $n+1$ is even. We now want to formalize what we mean by "and so on." Induction relies on the fact that if a property is valid for 1, and whenever it is valid for n it is also valid for $n+1$, then it must be valid for all numbers. The setup is as follows:

(1) We have a statement S_n about a natural number n (like "n is either even or odd")
(2) We know that
   (a) S_1 is true (this is sometimes called the **base case**), and that
   (b) if S_n is true, then S_{n+1} is true (this is sometimes called the **inductive step**).

The **principle/axiom of mathematical induction** states that if (1) and (2) hold, then S_n is true for all n.

The idea of why this must hold is that if (1) and (2) hold, then in particular we know S_1 implies S_2, and S_2 implies S_3, and so on. This can be thought of by picturing each S_n as a domino piece, with S_1 being the first one and S_{n+1} being after S_n. In this picture induction states that all the pieces are going to fall once the first falls.

Student question: Can this method be applied for other sets of numbers, for example rational numbers?

Answer: Rational numbers are a bit tricky. Induction may be applied to natural numbers greater than some numbers n. However, if we consider integers we see that there is a problem in where the starting point is. The same problem applies to rational numbers. There are ways to circumvent this (for example by indicating a correspondence between the naturals and the rationals), however.

We now prove Theorem 4.1.

Proof of Theorem 4.1. We prove by mathematical induction on the natural number $n \geq 1$ the statement

$$S_n\text{: } n \text{ is either even or odd.}$$

Base case: If $n = 1$ then n is odd (since $1 = 2 \cdot 0 + 1$), so n is either even or odd. So S_1 holds.

Inductive step: Assume n is a natural number and S_n holds. Thus n is either even or odd. We consider the two cases separately.

- If n is even, then $n+1$ is odd (as seen in class).
- If n is odd, then $n+1$ is even (as seen in class).

Thus $n+1$ is either even or odd.

Student question: How do we know that two cases exhaust all the possibility?

Answer: The fact that we only have two cases here is a property of this particular statement. We could have a statement in which more work needs to be done (for example, proving that the remainder of division by 3 is either 0, 1, or 2).

Therefore S_{n+1} holds. By the principle of mathematical induction, S_n is true for all natural numbers. □

We will now consider another example.

Theorem 4.2. *For all natural numbers n we have that*

$$0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

One way to see it is to see that we can regroup the terms in the sum as $(0+n)+(1+(n-1))+(2+(n-2))+\cdots = n+n+n+\cdots$ and counting how many terms there are (this depends on the parity of n).

A useful way to denote summation is **sigma notation**, where we indicate a sum of the form $f(0)+f(1)+\cdots+f(n)$ as

$$\sum_{i=0}^{n} f(i).$$

In particular, Theorem 4.2 states that

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}.$$

We are now ready to prove our theorem.

Proof of Theorem 4.2. We prove by induction on the non-negative integer $n \geq 0$ the statement

$$S_n : \sum_{i=0}^{n} i = \frac{n(n+1)}{2}.$$

Base case: Assume $n = 0$. Then $\sum_{i=0}^{n} i = 0$ and $n(n+1)/2 = 0$, so that S_0 holds.

Inductive step: Assume n is a non-negative integer and S_n holds. Thus

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}.$$

Then

$$\begin{aligned}\sum_{i=0}^{n+1} i =&0+1+2+\cdots+n+(n+1)\\ =&\left(\sum_{i=0}^{n} i\right)+(n+1)\\ =&\frac{n(n+1)}{2}+(n+1) && \text{by } S_n \text{ (the \textbf{inductive hypothesis})}\\ =&\frac{n(n+1)+2(n+1)}{2}\\ =&\frac{(n+1)(n+2)}{2}\end{aligned}$$

Thus

$$\sum_{i=0}^{n+1} = \frac{(n+1)(n+2)}{2}.$$

Therefore S_{n+1} holds.

By the principle of mathematical induction, S_n is true for all non=negative integers n. □

Student question: It looks like the two steps are very different: in the base case you have to prove that S_n works for $n = 1$, whereas in the inductive step you don't need to prove that S_n is true for a given n, but it is enough to just assume it. Is this correct?

Answer: This is correct–the two steps of a proof by induction are very different.

Let us now go back to our initial theorem.

Theorem 4.3. *Any natural number $n \geq 2$ has a prime divisor.*

If we proved our proof by induction, our inductive step would need to snow that $n+1$ has a prime divisor based on the assumption that n does. However, we see that this is not practical. In fact, we would rather prefer to know that $(n+1)/2, (n+2)/3$ and so on have prime divisors (whenever they are integers). In particular, it would be great to be able to assume that S_k is true for all k such that $1 \leq k \leq n$. This is called the principle of **strong induction**. The setup is as follows:

Assume that

(1) S_1 is true
(2) If S_m is true for all $m < n$.

Then S_n is true.

We are now ready to prove Theorem 4.3.

Student question: How can we think of strong induction in terms of the domino picture?

Answer: The domino picture is useful only as an intuition aid–numbers are not *exactly* like domino pieces. In any case, we can think of strong induction as saying that if all domino pieces before the nth one have fallen, then n too will fall.

At any rate, if you are ever in doubt about whether to use induction or strong induction, use strong induction.

Student question: Does normal induction imply strong induction?
Answer: Yes.

primedivisor. We prove by strong induction the statement

$$S_n\text{: } n \text{ can be written as a product of primes.}$$

Base case: If $n = 2$, then 2 is prime, so n is a product of one prime. Therefore S_2 is true.
Inductive step: Assume $n \geq 3$, and assume that S_m holds for all $m < n$ such that $2 \leq m$. If n is prime, we are done. If not, we can write $n = ab$ for a, b integers such that $1 < a < n$ and $1 < b < n$. By S_a, a is a product of primes, i.e. $a = p_1 \cdots p_k$ for primes $p_1, \ldots, p_k$. By S_b, $b = q_1 \cdots q_\ell$ for primes $q_1, \ldots, q_\ell$. Therefore

$$\begin{aligned} n =& ab \\ =& p_1 \cdots p_k \cdot q_1 \cdots q_\ell . \end{aligned}$$

So n is a product of primes. Thus S_n is true. By induction, S_n is true for all n. □

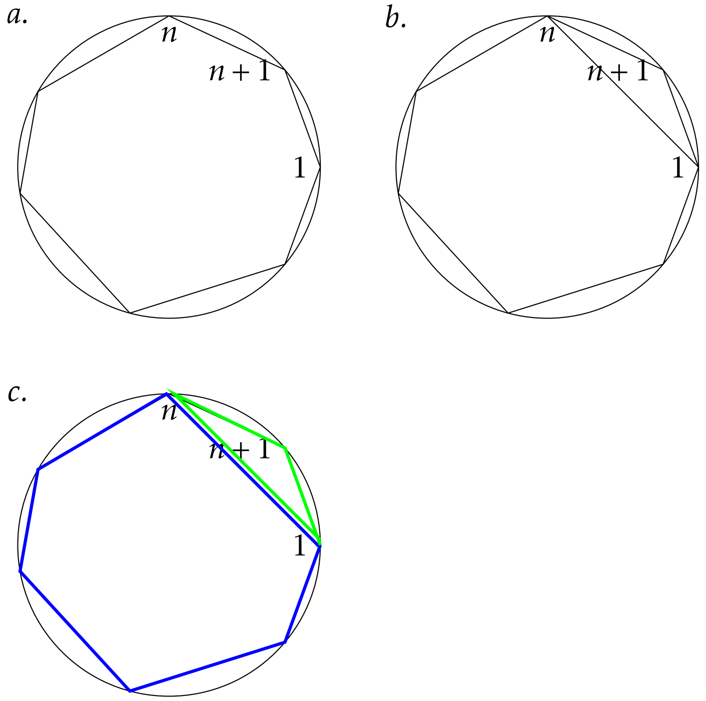
Student question: Where do you prove that S_m is true for all $m < n$?
Answer: We don't need to prove this; we just need to assume it.
An interesting exercise is to prove that given n points on a circle (where $n \geq 3$), the sum of the interior angles is $(n-2)180°$.

5. Friday, September 21

Last time we left with the following puzzle:

Prove that given n points on a circle (where $n \geq 3$), the sum of the interior angles is $(n-2)180°$.

A way to do it is to use induction. The base case for $n = 3$ is known. We now assume that it is true for n points. We now look at $n+1$ points, ordered counterclockwise. We then draw a line between point 1 and point n. The resulting figure is the union of an n-gon (in blue) and a triangle (in green). By the induction hypothesis we know that the sum of the angles of the n-gon is equal to $180(n-2)$, whereas that of the triangle is equal to 180. Therefore the total sum is equal to the sum of these two, which is equal to $180(n-1) = 180((n+1)-2)$. Thus the claim is proved by induction.



5.1. Sets.

Sets do not have a precise defition, but we can say that a **set** is a collection of (mathematical) things. For example, $\{1,8,3,7\}$ is a set. Order does not matter in a set, and thus the former set is the same as $\{8,7,1,3\}$. Two sets are the same when they have the same elements. There are some special sets:

- the **empty set**, denoted by $\emptyset$, is the set that cointains no elements;
- the set of natural numbers $\mathbb{N} = \{1,2,3,4,\dots\}$;
- the integers $\mathbb{Z} = \{\dots,-2,-1,0,1,2,\dots\}$;
- the rationals $\mathbb{Q}$;
- the reals $\mathbb{R}$.

These are sets that come up a lot and therefore are reserved a special notation.

If x is an element of A we write $x \in A$. For example,

- $1 \in \mathbb{N}$;
- $-1 \notin \mathbb{N}$;

- $\pi \in \mathbb{R}$;
- $\sqrt{2} \notin \mathbb{Q}$;
- $x \notin \emptyset$ for any x.

For a finite set A we define $|A|$ as the cardinality of A, i.e. the number of elements of A. For example, $|\emptyset| = 0$ and $|\{1,3\}| = 2$.

Sets don't have to contain numbers. For example, the set $V = \{a,e,i,o,u\}$ consisting of vowels in the English language is a set; so is the set $B = \{T,F\}$ contain true or false, the set $E = \{\{0,1\},\{1\}\}$ consisting of some sets, or even a mixed set of the form $\{\{1\},\pi,a\}$.

As a warning, note that $\{\emptyset\} \neq \emptyset$. In the homework you are going to see the set $\mathcal{P}(A)$ called the **power set** of A and defined as the set of all subsets of A. However, we still have not defined what a subset is.

Definition 5.1. Given two sets A and B we say that A is the **subset** of B, written $A \subseteq B$, if every element of A is an element of B.

For example, $\{1\} \subseteq \{1,\pi\}$, and $\emptyset \subseteq A$ for all sets A.

Note that we usually don't think about the set of all sets, since it can lead to paradoxes (Russel's paradox).

Now that we have the definition of a set we see that the power set of $\{1,2\}$ is the set

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

A useful case is to find a formula for the size of the power set of a set with n elements.

5.2. **Set builder notation.** We now have a limited notation for some special sets, such as the integers. However, consider the case where we might want to define the set E of even integers. Then the notation would look as follows:

$$\begin{aligned} E &= \{\underbrace{\ 2n\ }_{\text{expression}} \underbrace{|n \in \mathbb{Z}}_{\text{rule}}\} \\ &= \{\ldots,-4,-2,0,2,4,\ldots\} \\ &= \text{“the set of all objects of the form} \\ &\quad\ 2n\text{, for some integer } n\text{”} \\ &= \{x \in \mathbb{Z} | x = 2n \text{ for some integer } n\}. \end{aligned}$$

For example, consider the set $S = \{3k+1 | k \in \mathbb{N}\}$. We could also write this as $S = \{4,7,10,14,\ldots\}$. On the other hand, the set $\{1,3,5,7,\ldots\}$ can also be written as $\{2n+1 | n \in \mathbb{Z} \text{ and } n \geq 0\}$, or even just $\{x \in \mathbb{N} | x \text{ is odd}\}$.

5.3. **Operations on sets.**

Definition 5.2. Given two sets, we define their **union** as

$$\begin{aligned} A \cup B &= \{x | x \in A \text{ or } x \in B\} \\ &= \text{the set of things in } A \text{ or in } B, \end{aligned}$$

and their **intersection** as

$$\begin{aligned} A \cap B &= \{x | x \in A \text{ and } x \in B\} \\ &= \text{set of things in both } A \text{ and } B. \end{aligned}$$

For example,

$$\begin{aligned}\mathbb{N}\cup\{0\} =& \{0,1,2,3,\dots\}\\ \{1,2\}\cup\{2\} =& \{1,2\}\\ \{1,2,4\}\cap\{2,5,9\} =& \{2\}\\ \emptyset\cap\{5,6\} =& \emptyset\\ \emptyset\cup\{5,6\} =& \{5,6\}.\end{aligned}$$

Definition 5.3. Given sets A and B we define their **difference** as

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

For example, $\{1,5\} - \{5,3\} = \{1\}$.

Definition 5.4. Given sets A and U, we define the **complement** of A with respect to U, written A^c or $\overline{A}$, is the set $U - A$.

For example, if A is the set of even integers and $U = \mathbb{Z}$ then A^c is the set of odd integers. However, if $U = \mathbb{R}$ we have that $A^c = \{$ odd integers $\} \cup (\mathbb{R} - \mathbb{Z})$. Thus the complement of a set really depends on two sets. The set U is usually called the **universal set**.

For finite unions and intersection, we can use shorthand notations such as

$$\{1\}\cup\{2\}\{3\}\cup\cdots = \bigcup_{n\in\mathbb{N}}\{n\}$$
$$(-1,1)\cap\left(-\frac{1}{2},\frac{1}{2}\right)\cap\left(-\frac{1}{3},\frac{1}{3}\right)\cap\cdots = \bigcap_{n\in\mathbb{N}}\left(-\frac{1}{n},\frac{1}{n}\right).$$

In general, our sets need not be indexed by natural numbers, but we can have something as

$$\bigcup_{i\in I} A_i,$$

meaning the set of elements x that are in *some* A_i, and analogously the set

$$\bigcap_{i\in I} A_i$$

of elements that are in *all* the A_i's.

5.4. **Proving things about sets.** One of the most common things in proving things about sets is to prove that a certain element belongs to a set. To see how to do so we need to go back to the definition of A. For example, consider if we wanted to prove that

$$x \in \{y \in \mathbb{Z} : \text{ there is } n \in \mathbb{N} \text{ with } y = 5n+1\}.$$

To do this, we have to prove that

- $x \in \mathbb{Z}$, and

- There is $n \in \mathbb{N}$ with $x = 5n + 1$.

Another common procedure is to prove that $A \subseteq B$ for two sets A, B. To do so we must prove that if $x \in A$, then $x \in B$. A direct proof of this would start by assuming that $x \in A$ and concluding that $x \in B$.

A related thing is to prove that $A = B$, for which we first prove that $A \subseteq B$ and then that $B \subseteq A$.

An example of a theorem about sets is the following:

Theorem 5.5. *For sets A, B, C, we have that*

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

Proof. We first prove

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

Assume that $x \in A \cup (B \cap C)$. Then $x \in A$ or $x \in B \cap C$. We can address these cases separately.

If $x \in A$, then $x \in A \cup B$ and $x \in A \cup C$. So $x \in (A \cup B) \cap (A \cup C)$.

If $x \in B \cap C$, then $x \in B$ and $x \in C$ and therefore $x \in (A \cup B)$ and $x \in (A \cup C)$, which implies that $x \in (A \cup B) \cap (A \cup C)$. Therefore

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

The rest of the proof (the reverse inclusion) is left as an exercise. □

6. Monday, September 24

6.1. **Relations.** Last time we discussed sets, which are unordered collections of objects. Today we will study **relations**. We will see that relations are going to be defined as **ordered pairs**, i.e. lists of two things in which the order *does* matter. Examples of oder pairs include $(1,2), (1,1), (a,b), (\emptyset, \{\emptyset\}), (\text{red, black})$, and so on. In particular, $(1,2) \neq (2,1)$. Beyond ordered pairs, we can also look at n-**tuples**, which are ordered collections of n elements. For example, $(1,2,\pi)$ is a triple (3-tuple). Also note that $(1,2,2) \neq (1,2)$ whereas in the case of sets $\{1,2,2\} = \{1,2\}$.

We can also consider sets that are collections of ordered pairs, such as the set $\{(1,2),(1,1)\}$. In particular, the following is an important example of such a set:

Definition 6.1. The **cartesian product** of two sets A and B (written $A \times B$) is the set

$$\begin{aligned} A \times B = \{(a,b) | a \in A, b \in B\} \\ &= \text{set of all pairs with first component} \\ &= \text{in } A \text{ and second component in } B. \end{aligned}$$

Example 6.2. We see that

$$\{0,1\} \times \{1,3,4\} = \{(0,1),(1,1),(0,3),(1,3),(0,4),(1,4)\}.$$

Example 6.3. Another example that you might be familiar with is $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, which is the set of all points in the plane. We can also look at $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$, which is the set of points in 3-d space.

What do relations have to do with order? Relations are ways to relate two objects. For example an order $<$ on a set tells us if two elements are related with respect to some order. The same goes for $=$, and set membership $\in$, subset inclusion $\subset$, functions $y = f(x)$, and so on.

Student question: Are operations (addition, multiplication) relations?

Answer: That's a good question. Operations are similarly to relations, but have more than two arguments (some inputs and some outputs).

We now want to work with the general theory of relations. If we had to explain order to some alien that had no concept no order, how would we do it? One way is to just introduce a symbol, such as $<$, and specify what pairs can go at the sides of the symbol. For example, given the set $\{4,3,1,2\}$ we can introduce the symbol $<$ and specify that $1 < 2, 1 < 3, 1 < 4, 2 < 3, 2 < 4, 3 < 4$. This works for all relations: we can always specify pairs of elements that satisfy a certain relation (namely look at the *set* of all such pairs), and that's enough to specify what the relation is. For example, in our case order is given by the set

$$<= \{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}.$$

We could do the same with relations such as $\neq$, which would yield the set

$$\neq= \{(1,2),(1,3),(2,1),\dots\}.$$

We are going to use this as our definition of relation.

Definition 6.4. A **relation** on a set A is a subset R of $A \times A$. We write xRy if $(x,y) \in R$ and $x \not R y$ if $(x,y) \notin R$.

Student question: How can we draw relations, for example $\neq$?

Answer: We can draw arrows between related elements. Therefore the relation $\neq$ would connect all the elements but there would be no arrows from an element to itself. We can also draw it in terms of the cartesian product. Given the usual picture of the cartesian product, the relation $\neq$ consist of all the elements but those on the diagonal.

Example 6.5. Consider the set $\{1,2,3\}$ and the relation $\{(1,3),(3,1),(2,2),(1,1),(3,3)\}$. If we draw this we see that it connects odd numbers to odd numbers and even numbers to even numbers. Therefore xSy if x and y have the same parity.

In any case, relations need not have a definite meaning, and they need not be necessarily about numbers. The set $A = \{1,2,\emptyset\}$ with the relation $R = \{(1,\emptyset),(2,1),(1,2)\}$ does not have any apparent meaning to it, although it is still a relation.

Student question: So a relation is just an ordered set of pairs?

Answer: A relation is an *unordered* set. It does not matter what order you list related pairs.

Student question: Can a relation have more than two arguments?

Answer: Although we are only looking as binary relations, we can define n-ary relations with n arguments.

When we discussed relations earlier we mentioned relations such as $\in$. This does not fit our definition, since the left hand side of the relation is not in the same set of the right hand side. We introduce a definition to make up for this:

Definition 6.6. A **relation from** A **to** B is a subset R of $A \times B$.

Example 6.7. Consider the set $A = \{1,2\}$ and its power set $\mathcal{P}(A) = \{\emptyset,\{1\},\{2\},\{1,2\}\}$. The relation $R = \{(1,\{1\}),(1,\{1,2\}),(2,\{2\}),(2,\{1,2\})\}$ is a relation from A to $\mathcal{P}(A)$. This relation is actually $\in$. If we did not have a notion of membership, this would be the rigorous way to define it.

6.2. **Functions.** Relations can be used to describe functions. Consider the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$. We can plot it on the plane $\mathbb{R}^2$, which means that we can see it as a subset of $\mathbb{R} \times \mathbb{R}$. But this means that it is a relation! In fact, we see that for instance $(1,1),(2,4) \in f$. In particular, we can write its graph as

$$\left\{(x,x^2) | x \in \mathbb{R}\right\} \subset \mathbb{R} \times \mathbb{R}.$$

This works for any function, so every function is a relation. Is every relation a function? We see that in a relation there could be two pairs that share the first argument. This would be bad for a function, because you always want a function to have only one output for each input. To distinguish when a relation is a function, we introduce the following definition:

Definition 6.8. A **function** from A to B (written $f : A \to B$) is a relation from A to B satisfying the following condition: for every $a \in A$ thee is exactly one $b \in B$ such that $(a,b) \in f$. We abbreviate $(a,b) \in f$ by $f(a) = b$. The set A is called the **domain** and B is the **codomain**.

Remark. Note that a function is a relation between two sets, i.e. the input and the output can be from different sets.

Example 6.9. Consider the function $f(x) = 1/x$. This is a function from $\mathbb{R} - \{0\} \to \mathbb{R}$, i.e. $f : \mathbb{R} - \{0\} \to \mathbb{R}$. Is every element of the codomain an output of something? We see that 0 is not an output, and we are going to talk about these things when we talk about the range of a function.

Example 6.10. Consider $A = \{\emptyset, 1, 5\}$ and $B = \{3, 4, 6\}$. We can define the function

$$f = \{(1,3), (5,6), (\emptyset, 6)\}.$$

Another definition of this function would be given by

$$f(1) = 3, \quad f(5) = 6, \quad f(\emptyset) = 6.$$

Example 6.11. Let $A = B = \mathbb{R}$ and consider the relation

$$R = \left\{(x,y) \in \mathbb{R} \times \mathbb{R} | y = x^2\right\}.$$

This is a function, since for every x there is exactly one y such that $y = x^2$.

Proof. Assume $a \in \mathbb{R}$. Then take $b \in a^2$. Then $(a,b) \in R$. This shows that there is x such that $(a,x) \in R$. To show uniqueness, assume that $(a,c) \in R$. Then $c = a^2$ by definition of R, and therefore $c = b$. □

Example 6.12. Consider $S = \left\{(x,y) \in \mathbb{R} \times \mathbb{R} | y^2 = x\right\}$. This is *not* a function, since for each x there are two numbers y such that $y^2 = x$, namely $y = \sqrt{2}$ and $y = -\sqrt{2}$. We can see this by drawing a graph: in fact, the negative x axis has no output, and the positive x axis has two outputs.

Student question: Can you say that the output of a negative number is imaginary?

Answer: In this case since the codomain is $\mathbb{R}$ we can just say that negative values of x have no outputs.

7. Friday, September 28

7.1. **Equivalence relations.**

We are going to start by defining some properties that some relations can have.

Definition 7.1. Assume R is a relation on a set A. We say that R is

(1) **reflexive** if for any $x \in A$, xRx;
(2) **symmetric** if for any $x, y \in A$, if xRy then yRx.
(3) **transitive** if for any $x, y, z \in A$, if xRy and yRz then xRz.

Example 7.2. Consider the following relations on the set $A = \mathbb{Z}$.

	$<$	$\leq$	$=$	divides	$\neq$	does not divide	
reflexive	no	yes	yes	yes	no	no	
symmetric	no	no	yes	no	yes	no	
transitive	yes	yes	yes	yes	no	no	

If we look at the graph of a relation, we can try to determine the propertie of the relation by looking at the graph. For instance, a relation is reflexive if and only if for every point there are arrows from a point to itself; it is symmetric if every arrow goes both ways; it is transitive if for every three points x, y, z, if there is an arrow from x to y and from y to z then there is an arrow from x to z (note that it could be that $x = z$).

Yet another example of a relation is the following:

Definition 7.3. Assume n is a natural number and x and y are integers. We say that x is **congruent to y (modulo n)** (written $x \equiv y \mod n$) if n divides $x - y$.

Example 7.4. For example,

$$\begin{aligned} 0 &\equiv 2 \mod 2 \\ 0 &\not\equiv 1 \mod 2 \\ 1 &\equiv 5 \mod 2. \end{aligned}$$

We see that two numbers are congruent modulo 2 if and only if they have the same parity. Other examples include

$$\begin{aligned} -3 \equiv 0 \equiv 3 \equiv \cdots \equiv 9 \equiv \cdots &\mod 3 \\ 1 \equiv 4 &\mod 3 \\ 4 \equiv 1 &\mod 3. \end{aligned}$$

We might wonder if this relation is reflexive, symmetric, or transitive. In fact, it is all of the above.

Theorem 7.5. *Assume $n \in \mathbb{N}$. Then the relation $\equiv \mod n$ (on $\mathbb{Z}$) is reflexive, symmetric, and transitive.*

Proof. Reflexivity. Assume $x \in \mathbb{Z}$. Then

$$x - x = 0 = 0 \cdot n.$$

Since n divides 0, we have that n divides $x - x$, and by definition $x \equiv x \mod n$.

Symmetric. Assume $x, y \in \mathbb{Z}$, and assume that $x \equiv y \mod n$. By definition, it follows that n divides $x - y$. Therefore $x - y = an$ for some integer a. Then

$$y - x = -(x - y) = (-a)n$$

which means that n divides $y - x$. By definition, it follows that $y \equiv x \mod n$.

Transitive. Assume $x, y, z \in \mathbb{Z}$, and assume that $x \equiv y \mod n$ and $y \equiv z \mod n$. So n divides $x - y$ and n divides $y - z$. Therefore

$$x - y = an \quad y - z = bn$$

for some integers a, b. Adding the two equations we get that

$$x - z = (x - y) + (y - z) = (a + b)n.$$

So n divides $x - z$, and therefore $x \equiv z \mod n$. □

A relation that satisfies these properties has a special name:

Definition 7.6. A relation R on a set A is called an **equivalence relation** if it is reflexive, symmetric, and transitive.

Example 7.7. The relation $=$ on $A = \mathbb{Z}$ is an equivalence relation. As we just saw, the relation $\equiv \mod n$ on $A = \mathbb{Z}$ is an equivalence relation.

An important concept related to equivalence realtions is that of equivalence classes.

Definition 7.8. Assume R is an equivalence relation on a set A. Assume $a \in A$. The **equivalence class** of a is the set

$$[a] = \{x \in A | xRa\}.$$

Example 7.9. For the relation $\equiv \mod 3$, we see that the equivalence class of 1 contains $4, 7, 1, -2$, and so on. Similarly, $[2] = \{5, 8, 2, -1, \dots\}$ and $[3] = \{0, 3, 6, -3, \dots\}$. In particular, we see that $[4] = [1], [5] = [2], [6] = [3]$, and so on.

We might conjecture that there are only 3 equivalence classes. In fact, we see that if we consider the equivalence class of some n and this contains m, it looks like we should have that $[n] = [m]$. In fact, we can prove this.

Theorem 7.10. *Assume R is an equivalence relation in A. Assume $x, y \in A$. Then xRy if and only if $[x] = [y]$.*

We introduce the following definition in order to state the next theorem.

Definition 7.11. A **partition** P of a set A is a set of nonempty subsets of A whose union is A and such that the intersection of two distinct subsets in P is empty.

Theorem 7.12. *Assume R is an equivalence relation on A. Then*

$$\{[a] | a \in A\}$$

is a partition of A.

Proof of 7.10. Step 1: "if" direction. Assume $[x] = [y]$. By reflexivity, xRx and so $x \in [x]$. Therefore $x \in [y]$, and os xRy by definition of y.

Step 2: "only if" direction. Assume xRy. First we prove that $[x] \subset [y]$. Assume $a \in [x]$. Then aRx by definition of $[x]$ and xRy by assumption. Therefore aRy by transitivity, and so $[x] \subset [y]$. Second, we prove that $[y] \subset [x]$. Assume $a \in [y]$. Then aRy. Moreover, yRx by symmetry. Therefore aRx by transitivity and so $a \in [y]$. This proves that $[y] \subset [x]$, and in conclusion $[x] = [y]$. □

8. Monday, October 1

8.1. **Types of functions.**

Recall that a **function** from A to B (written $f : A \to B$) is a relation from A to B so that for each $x \in A$ there is exactly one $y \in B$ with $(x,y) \in f$ (written $f(x) = y$).

Example 8.1. Consider the sets $A = \{1,2,3\}$ and $B = \{4,5,6\}$. Consider the function $f : A \to B$ such that

$$f(1) = 4 = f(2), \quad f(3) = 5.$$

Note that we could have $x_1 \neq x_b$ with $f(x_1) = f(x_2)$ (in our previous example, take $x_1 = 1, x_2 = 2$). We could also have one $y \in B$ so that there is no $x \in A$ with $f(x) = y$ (here $y = 6$ has no $x \in A$ with $f(x) = 6$).

Definition 8.2. Assume $f : A \to B$ is a function. Then

(1) f is called **injective** when for $x_1, x_2 \in A$ if $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$ (in other words, "different imputs imply different outputs");
(2) f is called **surjective** if for all $y \in B$ there is $x \in A$ such that $f(x) = y$ (in other words, "each value in the codomain is an output");
(3) f is called **bijective** if it is both injective and surjective.

Example 8.3. With A and B as in the previous example, the function $f(1) = 4, f(2) = 5, f(3) = 6$ is bijective. However, if we add an element, say 3, to the set B, then f is not surjective anymore.

Assume A and B are finite., and assume that $f : A \to B$ is an injection. What can you say about $|A|$ and $|B|$? What if f is a surjection? Let's consider the case where f is an injection. Then we claim that $|A| \leq |B|$. Informally, we can think of an injection as a way of "copying" A into B, and therefore B must be able to contain it. If f is a surjection then $|A| \geq |B|$. In fact, if B was bigger than A, there would be not enough inputs to reach all the elements of B.

Example 8.4. Let $f : \mathbb{R} - \{0\} \to \mathbb{R}$ defined by

$$f(x) = \frac{1}{x} + 1.$$

Is it injective? We claim that it is.

Proof that f is injective. Assume $x_1, x_2 \in \mathbb{R} - \{0\}$. We prove the contrapositive, namely we prove that if $f(x_1) = f(x_2)$ then $x_1 = x_2$. Assume $f(x_1) = f(x_2)$. Then

$$\frac{1}{x_1} + 1 = \frac{1}{x_2} + 1.$$

So $1/x_1 = 1/x_2$. Multiplying both sides by $x_1 x_2$ we conclude that $x_2 = x_1$. □

Is f surjective? We claim that it is not. In order to prove that a function is not surjective, often we need to provide a value which is not an output.

Proof that f is not surjective. Take $y = 1$. Assume for a contradiction that there is $x \in \mathbb{R} - \{0\}$ such that $f(x) = y$. So

$$\frac{1}{x} + 1 = 1$$

and therefore $1/x = 0$, which is a contradiction. □

Example 8.5. Consider

$$\begin{aligned} g : \mathbb{R} - \{0\} &\to \mathbb{R} - \{1\} \\ g(x) &= \frac{1}{x} + 1. \end{aligned}$$

Then g is injective as before. We claim that it is surjective.

Proof. Assume $y \in \mathbb{R} - \{1\}$. Take $x = 1/(y-1)$. This is well-defined since $y - 1 \neq 0$. Then

$$\frac{1}{x} + 1 = \frac{1}{\frac{1}{y-1}} + 1 = y - 1 + 1 = y$$

and therefore $g(x) = y$. □

Example 8.6. Take

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R}^2 \\ f(x) &= x^2. \end{aligned}$$

Then f is not injective, since $f(-1) = f(1) = 1$. It is also not surjective, since there is no $x \in \mathbb{R}$ such that $x^2 = -1$.

Example 8.7. Take

$$\begin{aligned} g : \mathbb{R}_{\geq 0} &\to \mathbb{R}_{\geq 0} \\ g(x) &= x^2. \end{aligned}$$

Then g is bijective. Note that this is the same function as before, but changing the domain made it injective and changing the codomain made it surjective.

Example 8.8. Let

$$\begin{aligned} g : \{ \text{ people on earth } \} &\to \{ \text{ days of the year } \} \\ g(x) &= \text{birthday of } x. \end{aligned}$$

We see that this function is not injective and it is surjective. If we change the domain to people in this class, it is not surjective and it is injective, defying the odds of the birthday paradox.

8.2. **Composition.**

Definition 8.9. Consider maps $f : A \to B$ and $g : B \to C$. The **composition** of f and g (written $g \circ f$) is a function $g \circ f : A \to C$ defined by

$$(g \circ f)(a) = g(f(a)).$$

Example 8.10. Let

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ f(x) &= x^2 \\ g : \mathbb{R} &\to \mathbb{R} \\ g(x) &= 1 + x. \end{aligned}$$

Then

$$\begin{aligned}(g\circ f)(x) =&1+x^2\\ (f\circ g)(x) =&(1+x)^2.\end{aligned}$$

Therefore the composition of two functions (even with the same domain and codomain) depends on the order of the composition.

Example 8.11. Consider $f : A \to B$ and $g : B \to C$. If both f and g are injective (resp. surjective), is $g \circ f$ injective (resp. surijective)? Consider the injective case first.

Proof that $g\circ f$ is injective. If $x_1, x_2 \in A$ are distinct, it follows that $f(x_1) \neq f(x_2)$ since f is injective. Therefore $g(f(x_1)) \neq g(f(x_2))$ since g is injective. Therefore $g \circ f$ is injective. □

Consider now the surjective case.

Proof that $g\circ f$ is surjective. Take $c \in C$. Then there exists $b \in B$ such that $g(b) = c$ since g is surjective. Then there exists $a \in A$ such that $f(a) = b$ since f is surjective. It follows that $(g \circ f)(a) = g(f(a)) = g(b) = c$ and therefore $(g \circ f)$ is surjective. □

8.3. **Inverse.** Suppose $f : A \to B$ is a bijection. Can we get a function that "goes back" from B to A? Consider $b \in B$. We claim that if f is bijective there is exactly one $a \in A$ such that $f(a) = b$. We know that there is *at least* one such a since f is surjective. If a_1 and a_2 both satisfy $f(a_1) = f(a_2) = b$ then $a_1 = a_2$ by injectivity. Therefore a is unique.

Definition 8.12. The **inverse** of a bijection $f : A \to B$ is the function

$$f^{-1} : B \to A$$

where $f^{-1}(b)$ is defined as the unique $a \in A$ such that $f(a) = b$.

What is $f \circ f^{-1}$? And what about $f^{-1} \circ f$? We see that

$$\begin{aligned}f\circ f^{-1} : B \to& B\\ (f\circ f^{-1})(b) =&b\\ f^{-1}\circ f : A \to& A\\ (f^{-1}\circ f)(a) =&a.\end{aligned}$$

9. Friday, October 5

9.1. **Cardinalities.** We saw last time that bijection create a correspondece between two sets. This implies that if A and B are finite sets and we have a bijection $A \to B$ then $|A| = |B|$, i.e. the sets have the same cardinality. Is the converse true? Namely, suppose that $|A| = |B|$. Is there a bijection $A \to B$? The answer turns out to be *yes*.

Proof. Suppose $n = |A| = |B|$. We can write $A = \{a_1, \dots, a_n\}$ and $B = \{b_1, \dots, b_n\}$. Define $f : A \to B$ by $f(a_i) = b_i$. This is a bijection. □

The point of the proof is that once you have a finite set you can number its elements, and then construct a bijection based on the numbering. At this point we might want to talk about sizes of infinite sets. We can't number infinite sets, so we are just going to define cardinality based on bijections.

Definition 9.1. Two sets A and B **have the same cardinality** if there is a bijection from A to B.

Note that we are not defining what the cardinality of a set is, but we are limiting ourselves to defining what it means for two sets to have the same cardinality.

Example 9.2. The relation "having the same cardinality" is an equivalence relation. First, we check it's reflexive. According to the definition, we must find a bijection from a set to itself. The identity works for this purpose, and therefore the relation is reflexive. We now check it's symmetric. If there is a bijection $f : A \to B$ between two sets A, B we want to prove that there is a bijection from B to A. This is the inverse $f^{-1} : A \to B$. We now check transitivity. Assume $f : A \to B$ and $g : B \to C$ are bijections. Last time we proved that $g \circ f : A \to C$ is a bijection. It follows that $(g \circ f)^{-1} : C \to A$ is a bijection, and therefore the relation is transitive. This concludes the proof.

We are now going to look at infinite sets and see whether they have the same size.

Example 9.3. Consider $A = \mathbb{N}$ and $B = \mathbb{N} \cup \{0\}$.

Theorem 9.4. *The sets A and B have the same cardinality.*

Proof. We define $f : A \to B$ by $f(n) = n - 1$. This is well defined since if $n \in \mathbb{N}$ then $n - 1$ is either 0 (if $n = 1$) or a natural number (if $n > 1$). We now prove it is injective. Assume $n, m \in \mathbb{N}$ such that $f(n) = f(m)$. This means that $n - 1 = m - 1$, and adding 1 to both sides we get that $n = m$. To prove that it is surjective, assume $y \in \mathbb{N} \cup \{0\}$. Take $x = y + 1$. Then $x \in \mathbb{N}$ and $f(x) = x - 1 = y + 1 - 1 = y$, and therefore f is surjective. □

Student question: Why do we care about the cardinality of an infinite set?

Answer: One answer is that it is philosophically interesting, and this is one of the historical reasons of the origin of the theory of cardinality. Another use is in computer science, where we want to number things. There are other uses in math, and different mathematicians will give different answers when asked the question.

Example 9.5. Hilbert's hotel is a hotel with an infinite number of rooms. One day every room has a guest in it, and a visitor comes to the hotel looking for a room. It is actually possible to find a room for the visitor by having all the guest occupy the next room.

Example 9.6. We can prove the following:

Theorem 9.7. *Take $A = \mathbb{N}$ and $B = \mathbb{Z}$. Then A and B have the same cardinality.*

The idea of the proof is that we start by mapping 1 to 0, 2 to 1, 3 to −1, 4 to 2, and so on. We want to formally prove how this works.

Proof. Define $f : A \to B$ by

$$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ -(n-1)/2 & \text{if } n \text{ is odd} \end{cases}.$$

We now prove that f is an injection. Assume that $n, m \in \mathbb{N}$ and $f(n) = f(m)$. We consider four cases depending on the parity of n and m.

Case 1: n is odd and m is odd. By definition of f, this implies that

$$-\frac{n-1}{2} = -\frac{m-1}{2}$$

and therefore $n = m$.

Case 2: n is even and m is even. Similarly to case 1, we have that

$$\frac{n}{2} = \frac{m}{2}$$

and therefore $n = m$.

Case 3: n is odd and m is even. We have that

$$-\frac{n-1}{2} = \frac{m}{2}.$$

Note that since $n \in \mathbb{N}$ it follows that

$$-\frac{n-1}{2} \leq 0.$$

Similarly, since $m \in \mathbb{N}$ we have that $m/2 > 0$. This means that the above equality is impossible, and thus this case is irrelevant.

Case 4: n is even and m is odd. Similar to case 3.

Having proved all cases, we conclude that f is injective.

We now prove f is surjective. Assume $y \in \mathbb{Z} = B$. We consider the cases where $y \leq 0$ and $y > 0$.

Case 1. $y \leq 0$. In this case take $x = -2y + 1$. Then $f(x) = y$.

Case 2. $y > 0$. Consider $x = 2y$. Then $f(x) = y$.

In conclusion, f is bijective. □

Example 9.8. The sets $\mathbb{N}$ and $\mathbb{Q}$ have the same cardinality. The idea of the proof is the following: fill a table

	0	1	-1	2	-2	3	-3
1	0/1	1/1	−1/1	2/1	⋯		
2	0/2	1/2	−1/2	⋯			
3	0/3	1/3	−1/3	⋯			
4	0/4	1/4	⋱				
5	⋮						

and count them in a criss-cross fashion. We could formalize this bijection, but it takes time.

At this point, one could start to think that all infinite sets are in bijection with the natural numbers. However, the next example disproves this.

Example 9.9. The sets $\mathbb{N}$ and $\mathbb{R}$ don't have the same cardinality.

Proof. Assume for a contradiction that there is a bijection from $\mathbb{N}$ to $\mathbb{R}$. By writing real numbers in their decimal expansion, we can write the bijection in a table

	$f(n)$
1	0.15321100...
2	5.33333...
3	18.9191919191534827...
4	3.1415926...
$\vdots$	$\vdots$

and try to create a real number which is not in the list. Define d_{ij} to be the ith digit after the decimal point of the number in the jth row. Define now $x = 0.d_{11}d_{22}d_{33}\ldots$ and define a new number $\bar{x} = 0.\bar{d}_{11}\bar{d}_{22}\bar{d}_{33}\ldots$ where

$$\bar{d}_{ii} = \begin{cases} 0 & \text{if } d_{ii} = 9 \\ d_{ii} + 1 & \text{if } d_{ii} \neq 9 \end{cases}.$$

In our case, $\bar{x} = 0.2406\ldots$ We now claim that $\bar{x}$ is not in our table above, i.e. is not in the image of the bijection. In fact, suppose $f(n) = \bar{x}$ for some n. But then this implies that $d_{nn} = \bar{d}_{nn}$, which is impossible. This is a contradiction, and therefore there is no bijections between $\mathbb{R}$ and $\mathbb{N}$. □

This procedure is called diagonalization (from the fact that we construct the number x by taking digits on the diagonal).

10. Friday, October 12

10.1. Group theory.

10.1.1. *Idea.* We already know mathematical structure with operations such as + and $\cdot$, such as $\mathbb{Z}$ and $\mathbb{R}$. We want to describe other places with similar operations. First, we have to define what an operation is.

Definition 10.1. A **binary operation** on a set A is a function $*: A \times A \to A$. We will write $a * b$ instead of $*(a, b)$.

Example 10.2. The operation + on $A = \mathbb{Z}, \mathbb{R}, \mathbb{N}$. However, + is not a binary operation on the set $\{1, 2\}$, since $1 + 2 \notin \{1, 2\}$.

Example 10.3. The operation max is a binary operation on $\mathbb{R}$ which takes two inputs a, b and outputs their maximum $\max(a, b)$.

Example 10.4. Another operation on $A = \mathbb{Z}$ could be something like $a * b = 5a + 7b$, or $a * b = a - b$. Note however that subtraction is not a binary operation on $A = \mathbb{N}$.

We are now ready to define a group.

Definition 10.5. A **group** is a set G with a binary operation $*$ on G satisfying three properties:

(1) $*$ is associative: if $a, b, c \in G$ then
$$(a * b) * c = a * (b * c);$$
(2) there exists $e \in G$ such that for any $a \in G$
$$e * a = a * e = a;$$
the element e is called the **identity element**;
(3) for any $a \in G$ there exists $b \in G$ such that
$$a * b = b * a = e;$$
we call b the inverse of a.

We write the group as $(G, *)$.

Remark. Note that property (2) is of the form "there exists . . . such that for all . . ." while property (3) is of the form "for all . . . there exists."

Example 10.6. Going back to our example, we see that $(\mathbb{Z}, +)$ is a group. The identity element is 0 and for $a \in \mathbb{Z}$ we know that $a + (-a) = 0$. The same goes for addition on $\mathbb{R}$. However, $(\mathbb{N}, +)$ is not a group, since it does not contain 0. Even $(\mathbb{N} \cup \{0\}, +)$ is not a group since it has no inverses. How about $(\mathbb{R}, \cdot)$? We see that properties (1) and (2) hold, but (3) does not since 0 has no inverse. In particular, $(\mathbb{R} - \{0\}, \cdot)$ is a group.

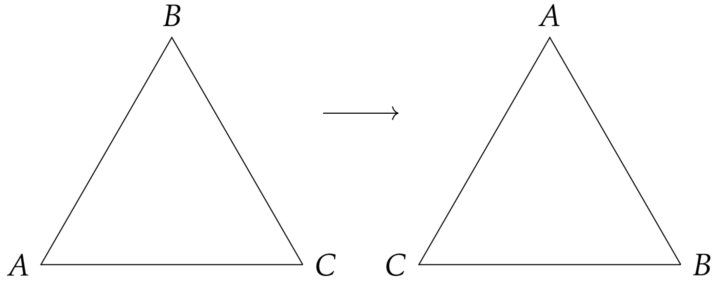
Student question: Can there be multiple identity elements?
Answer: We will see that the identity is unique.

Most of these groups we have seen are commutative, but this is not necessary:

Definition 10.7. A group G is **abelian** (or commutative) if $a * b = b * a$ for all $a, b \in G$.

Example 10.8. Consider the group of invertible 2×2 matrices with matrix multiplication as operation. This group is not abelian since there exist matrices that do not commute.

10.1.2. *Symmetries of an equilateral triangle.* In this case, a symmetry is a rigid transformation preserving the shape. This includes not doing nothing, rotating, and reflecting. In any symmetry, what counts is where each vertex goes. For example, the symmetry



is written $\left(\begin{smallmatrix} A & B & C \\ B & C & A \end{smallmatrix}\right)$ to indicate that A went where B was, B where C was, and C where A was. We can see these as functions (e.g. mapping A to B and so forth) so that we can write composition of symmetries as $\circ$ (this is the group operation). We can list all of the symmetries and give them a name:

$$\begin{aligned}
\mathrm{id} &= \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} \\
\rho_1 &= \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix} \\
\rho_2 &= \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} \\
\mu_1 &= \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} \\
\mu_2 &= \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} \\
\mu_3 &= \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}.
\end{aligned}$$

A way we can understand this group better is by writing a multiplication table:

$\circ$	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
id	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	id	μ_3	μ_1	μ_2
ρ_2	ρ_2	id	ρ_1	ρ_2	ρ_3	ρ_1
μ_1	μ_1	$\cdots$				
μ_2	$\vdots$	$\ddots$				
μ_3						

We need to check that this is a group. We know that function composition is associative, and we see that the identity symmetry is the identity of this operation. Moreoever, the inverse of ρ_1 is ρ_2 (and vice versa) and the inverse of μ_i is itself (for $i = 1,2,3$).

10.1.3. *Basic properties of groups.* We are mainly going to study groups abstractly; even so, there are several useful properties of groups that we can prove.

Proposition 10.9. *There is a unique identity element.*

Proof. We need to show that an identity exists, and that there is at most one identity. We already know that e exists by definition of groups. Assume now e, e' are identity elements. Since e is the identity it follows that $e * e' = e'$, and since e' is the identity it follows that $e * e' = e$. Therefore $e = e'$. □

Proposition 10.10. *Each element has a unique inverse.*

Proof. We know by the definition that there is at least one inverse. We now prove there is at most one. Assume $a \in G$ and $b, b' \in G$ are inverses of a (namely, $a * b = b * a = e$ and $a * b' = b' * a = e$). Therefore

$$b = b * e = b * (a * b') = (b * a) * b' = e * b' = b'$$

and so $b = b'$. □

In what follows, we will write the inverse of $a \in G$ as a^{-1} and we will suppress the operation symbol $*$.

Proposition 10.11. *For all $a, b \in G$ we have that*

$$(ab)^{-1} = b^{-1}a^{-1}.$$

Proof. We need to prove that

$$\begin{aligned}(ab)\left(b^{-1}a^{-1}\right) &= e\\ \left(b^{-1}a^{-1}\right)(ab) &= e.\end{aligned}$$

By associativity we have that

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e.$$

We prove the other equation similarly. □

11. Monday, October 15

Student question: I read that a group needs to be closed under the group operation. Do we not require that?

Answer: We require closure under our operation when we specify that $*$ is a map from $G \times G$ to G.

Student question: Can you repeat elements when writing down a group?

Answer: The underlying set of a group is a set, and therefore the usual set notation applies; in particular one can repeat elements.

11.1. Subgroups.

The idea behind subgroups is that they are the "parts" of a group.

Definition 11.1. A **subgroup** of a group $(G,*)$ is a subset $H \subset G$ that is also a group under $*$. Equivalently:

(1) $e \in H$;
(2) if $a, b \in H$ then $a * b \in H$;
(3) if $a \in H$ then $a^{-1} \in H$.

Example 11.2. The even integers are a subgroup of $(\mathbb{Z},+)$. We can check this in several ways. For example, we can check that it contains the identity 0, that it is closed under $+$ (we proved this in one of the first classes) and given an even number its negative is also even. Note that in this case we might write 2^{-1} as the inverse of 2, but this does not mean that $2^{-1} = 1/2$ because the operation is addition.

Example 11.3. On the other hand, $\mathbb{N} \cup \{0\}$ is not a subgroup of $(\mathbb{Z},+)$ since $-1 \notin \mathbb{N} \cup \{0\}$.

Example 11.4. The set of 2×2 matrices of determinant 1 is a subgroup of the invertible 2×2 matrices.

Example 11.5. Given any group G, then $H = G$ is a subgroup, and $H = \{e\}$ is also a subgroup.

Example 11.6. In the homework you saw that bijections from $\mathbb{N}$ to $\mathbb{N}$ form a group. This is because every bijection has an inverse function, and this is the inverse of the group operation; moreover, the identity function is the identity under the group operation. In fact, for any set A the set of bijections from A to A is a group. It is so important that in the case of finite sets it has a name.

Definition 11.7. For $n \in \mathbb{N}$ the group of bijections from $\{1,2,\dots,n\}$ to $\{1,2,\dots,n\}$ under composition is denoted S_n and is called the **symmetric group**.

Example 11.8. Let $n = 4$. Then an element of S_4 is a map

$$\sigma : \{1,2,3,4\} \to \{1,2,3,4\}.$$

For example, we might have $\sigma(1) = 2$, $\sigma(2) = 4$, $\sigma(3) = 3$, $\sigma(4) = 1$. We can write this as

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}.$$

It is easier to think of members of S_n as permutations (ways to rearrange n things) rather than just bijections.

Example 11.9. Going back to the previous example, let's calculate σ^2. We can check that

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}.$$

What about σ^3? We find that

$$\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

This means that $\sigma^3 = e = \mathrm{id}$.

Definition 11.10. The **order** of an element $a \in G$ is the minimal $n \in \mathbb{N} \cup \{0\}$ such that $a^n = e$ (or ∞ if such n does not exist).

Definition 11.11. The **order** of a group G is the number of elements in the group.

Example 11.12. What is the order of the group S_n? We want to list all the possible bijections from $\{1, 2, \dots, n\}$ to itself; therefore, we must first specify where 1 is sent. There are n ways to specify this. After this, we have $(n-1)$ ways to specify where 2 is sent, and so on until we have only 1 way to specify where n is sent. Therefore the number of bijections is equal to $n \cdot (n-1) \cdots 2 \cdot 1$. This number is also written as $n!$ and is called n **factorial**. For example, $|S_4| = 24$ and $|S_3| = 6$.

Last time we studied the group of symmetries of an equilateral triangle. This is a subgroup of S_3, since it permutes 3 things. Since it has the same number of elements as S_3, it turns out that it is the same group as S_3.

11.1.1. *Symmetries of an n-gon.*

Definition 11.13. Let D_n denote the group of simmetries of an n-gon for $n \geq 3$.

Example 11.14. What are the elements of D_4? We can list all of them. The group contains the identity that does not change anything. It also contains rotations (and they form a subgroup). We can also flip the square, which gives us other elements. Since every symmetry of the square is specified by knowing where one vertex went and whether there was a flip, the order of D_4 is $|D_4| = 8$. In particular, D_4 is a proper subgroup of S_4 (where "proper" means that $D_4 \neq S_4$).

Example 11.15. Consider now the subset of S_4 defined by

$$H = \{\sigma \in S_4 | \sigma(1) = 1\}.$$

This group is actually analogous to S_3, since we only permuting 3 elements. However, it is not quite the same thing as S_3, since the elements are not the same.

Theorem 11.16. *The order of D_n is equal to $|D_n| = 2n$.*

Proof. Given an n-gon, an element of D_n has n ways to send the vertex 1 to some other vertex. Since it must preserve the n-gon, the vertex 2 cannot be sent wherever we want; rather, there are only 2 possible choices for where vertex 2 is sent. After this, all the other vertices are determined. Therefore $|D_n| = 2n$. □

Theorem 11.17. *Any element of D_n can be written as a product of r and s where*

$$r = \begin{pmatrix} 1 & 2 & \cdots & n \\ n & 1 & \cdots & n-1 \end{pmatrix}$$

(a rotation) and s is the reflection fixing 1.

Is the group D_n abelian? We can check that $rs \neq sr$ and therefore D_n is not abelian.

12. Friday, October 19

12.1. **Group morphisms.** Today we are going to look at two groups that are very similar. In the homework you saw the group $(\mathbb{Z}_2, 2)$. Its underlying set is $\mathbb{Z}_2 = \{[0],[1]\}$ with the operation given by

+	[0]	[1]
[0]	[0]	[1] .
[1]	[1]	[1]

However, we can also look at the group with underlying set $\{1,-1\}$ and operation given by

·	1	-1
1	1	-1 .
-1	-1	1

We see that both these group look the same since their table is given by

	e	a
e	e	a .
a	a	e

In fact, it does not really matter what the underlying sets of the groups are; what matters is the structure. Another example is the following: consider the group of bijections from the set $\{1,2,3\}$ to itself. This is the same as the group of bijections from the set $\{A,B,C\}$ to itself, or from $\{4,5,6\}$ to itself, and so on. This is because it does not matter what the elements are, as long as there are 3 of them. This concept is encapsulated in the following definition.

Definition 12.1. Assume $(G,*_G)$ and $(H,*_H)$ are groups. We say that they are **isomorphic** if there exists a bijection $\rho : G \to H$ that preserves the group operation. Namely, for any $a,b \in G$ we must have that

$$\rho(a *_G b) = \rho(a) *_H \rho(b).$$

We say that ρ is called an **isomorphism** from $(G,*_G)$ to $(H,*_H)$.

Example 12.2. Define $\rho : \mathbb{Z}_2 \to \{1,-1\}$ by

$$\begin{aligned}\rho([0]) =& 1\\ \rho([1]) =& -1\end{aligned}$$

. We claim that this is an isomorphism.

Proof. This is clearly a bijection. We now check that this is a group operation. We do so by checking all possible values.

$$\begin{aligned}f([0]+[0]) =& f([0]) = 1 = 1 \cdot 1 = f([0]) \cdot f([0])\\ f([0]+[1]) =& f([1]) = -1 = 1 \cdot (-1) = f([0]) \cdot f([1])\\ f([1]+[0]) =& f([1]) = -1 = (-1) \cdot 1 = f([1]) \cdot f([0])\\ f([1]+[1]) =& f([0]) = 1 = (-1) \cdot (-1) = f([1]) \cdot f([1]).\end{aligned}$$

Thus f is an isomorphism. □

What if I had tried another bijection, such as $g([0]) = -1$ and $g([1]) = 1$? This is a bijection, but it does not preserve the operation: in fact,

$$g([0]+[0]) = g([0]) = -1 \neq 1 = (-1)\cdot(-1) = g([0])\cdot g([0]).$$

Example 12.3. Let's look at $(\mathbb{Z}_3, +)$. We claim that this is isomorphic to the group H of rotations of an equilateral triangle. We denote the latter by $\left(\left\{\mathrm{id}, r, r^2\right\}, \circ\right)$ where r is a clockwise rotation of 120° (this is a subgroup of D_3). One way we can do this is to define an explicit bijection, for example $f([0]) = \mathrm{id}, f([1]) = r, f([2]) = r^2$. The next step would then be to check all 6 cases. Another way is the following: we define

$$f([a]) = r^a,$$

with the convention that $r^a = \mathrm{id}$. Note that this is actually valid for any integer a since $r^3 = \mathrm{id}$ and so we only care about the class of a in $\mathbb{Z}_3$. The function f is clearly a bijection, and we now show that it preserves the group operation. In fact, assume $a, b \in \mathbb{Z}$. Then

$$f([a]+[b]) = f([a+b]) = r^{a+b} = r^a \circ r^b = f([a]) \circ f([b]).$$

Thus this is an isomorphism. One can check that the bijection defined by $g([0]) = \mathrm{id}, g([1]) = r^2, g([2]) = r$ is also an isomorphism. This is because r^2 is the same as a counterclockwise 120° rotation, and thus the groups are the same for all practical purposes.

Example 12.4. Consider the groups $(\mathbb{Z}_2, +)$ and $(\mathbb{Z}_3, +)$. These cannot be isomorphic, since the underlying sets have different cardinalities (that is to say, the groups have different order).

Last week we saw that bijections defined an equivalence relation. Does this work for isomorphisms too? Namely, is it true that the relation "being isomorphic" is an equivalence relation? This is left as an exercise.

Example 12.5. Consider $(\mathbb{Z}_6, +)$ and D_3. Both groups have 6 element, so there are bijections between them. However, it turns out that they are not isomorphic. There are many ways to check this. One proof is as follows:

Proof. Assume for a contradiction that $f : \mathbb{Z}_6 \to D_3$ is an isomorphism. Write $D_3 = \left(\left\{\mathrm{id}, r, r^2, s, s_2, s_3\right\}, \circ\right)$ where the last elements are the reflections. Pick $a, b \in \mathbb{Z}_6$ such that $f(a) = s_1$ and $f(b) = s_2$ (these exist since f is surjecive). Since $s_1^2 = \mathrm{id}$ we must have that either $a = 0$ or $a = 3$. But f is injective and 0 goes to id, and so it must be that $a = 3$. But the same goes for b, which is a contradiction since f is supposed to be a function. □

Another proof is the following:

Proof. The group $\mathbb{Z}_6$ is abelian, but the group D_3 is not. It follows that they cannot be isomorphic. □

The last proof involved something that we are going to prove in general.

Theorem 12.6. *If f is an isomorphism from $(G, *_G)$ to $(H, *_H)$ and $(G, *_G)$ is abelian, then $(H, *_H)$ is abelian.*

Proof. Assume $b_1, b_2 \in H$. Since f is a surjection we can pick $a_1, a_2 \in G$ such that $f(a_1) = b_1$ and $f(a_2) = b_2$. Since G is abelian, $a_1 *_G a_2 = a_2 *_G a_1$. So $f(a_1 *_G a_2) = f(a_2 *_G a_1)$. Therefore, since f preserves the operation it follows that

$$b_1 *_H b_2 = f(a_1) *_H f(a_2) = f(a_2) *_H f(a_1) = b_2 *_H b_1.$$

Therefore H is abelian. □

We don't have to look at finite groups. The following example is about infinite groups.

Example 12.7. We claim that $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$, with the isomorphism give by $f(x) = e^x$. This is a bijection since e^x is injective and its image is $\mathbb{R}_{>0}$. Moreover, it preserves the group structure since

$$f(a+b) = e^{a+b} = e^a \cdot e^b = f(a) \cdot f(b).$$

There is a generalization of group isomorphisms that covers the case where the function is not a bijection.

Definition 12.8. Consider a function $f : G \to H$. We say that f is a **homomorphism** if f is a function preserving the group operation.

Example 12.9. The map $\mathbb{Z} \to \mathbb{Z}_n$ defined by

$$f(a) = [a]$$

is a homomorphism. Note that f is not injective.

Example 12.10. The determinant defines a homomorphism between invertible matrices and $(\mathbb{R} - \{0\}, \cdot)$, since given matrices A, B we have that $\det(AB) = \det(A) \cdot \det(B)$.

Example 12.11. The absolute value map

$$|-| : (\mathbb{R} - \{0\}, \cdot) \to (\mathbb{R}_{>0}, \cdot)$$

is a homomorphism since $|x||y| = |xy|$. As before, this is not injective.

Student question: Does "being homomorphic" define an equivalence relation?
Answer: In fact, any two groups are homomorphic, since we can always define a map $f : (G, *_G) \to (H, *_H)$ such that $f(a) = e_H$. The latter is a homomorphism, and therefore the equivalence relation defined by being homomorphic is not used as it is not very useful.

As in linear algebra, we can define the **kernel** and **image** of a homomorphism as

$$\begin{aligned} \ker(f) &= \{a \in G | f(a) = e_H\} \\ \operatorname{im}(f) &= \{b \in H | \text{ there exists } a \in G \text{ such that } f(a) = b\}. \end{aligned}$$

The following is a very useful result:

Theorem 12.12. *If $f : G \to H$ is a homomorphism, then $f(e_G) = e_H$.*

Proof. We know that

$$f(e_G) = f(e_G *_G e_G) = f(e_G) *_H f(e_G).$$

Therefore

$$e_H *_H f(e_G) = f(e_G) = f(e_G) *_H f(e_G).$$

So

$$e_H *_H f(e_G) = f(e_G) *_H f(e_G)$$

and therefore $e_H = f(e_G)$. □

13. Monday, October 22

13.1. **Cyclic groups.** The motivation for cyclic groups is that we want to study not only $(\mathbb{Z}, +)$ but also $(\mathbb{Z}_n, +)$. If we wanted to draw a picture of $\mathbb{Z}$, we would come up with something like a line, and adding $+1$ will make us go one step right on this line. Similarly, adding -1 will make us go one step left; by doing these two things (adding or subtracting 1) will yield all the elements in this group. If we wanted to draw $\mathbb{Z}_n$, then instead of a line we would get something like a circle. For example, for $n = 12$ we would get an analog clock. In this case we can get to every element by just adding 1. Last time we saw that $\mathbb{Z}_3$ is isomorphic to the group of rotations of the triangle, and in this case it was important that one could get any element starting by one particular element. We want to formalize this concept of "get to every element of $\mathbb{Z}_n$ by adding 1."

Definition 13.1. Assume G is a group, and let $a \in G$. Define

$$\langle a \rangle = \{a^n | n \in \mathbb{Z}\}.$$

We call this the **cyclic subgroup generated by** a.

Recall that for $n \in \mathbb{N}$ we write

$$a^n = \underbrace{aaa \cdots a}_{n \text{ times}}$$

with the convention that $a^0 = e$ and

$$a^{-n} = \left(a^{-1}\right)^n = \underbrace{a^{-1}a^{-1} \cdots a^{-1}}_{n \text{ times}}.$$

Note that in groups where the operation is $+$, when we write a^n we really mean na. For example, in $G = (\mathbb{Z}, +)$ we would have that $3^2 = 6$. Therefore we have that in this case

$$\langle e \rangle = \{0 \cdot 3, 1 \cdot 3, (-1) \cdot 3, 2 \cdot 3, \dots\} = \{3n | n \in \mathbb{Z}\}.$$

Similarly, $\langle 0 \rangle = \{0\}$ and $\langle 1 \rangle = \mathbb{Z}$. We now prove that cyclic subgroups are in fact subgroups.

Theorem 13.2. *Assume G is a group and let $a \in G$. Then the set $H = \langle a \rangle$ is a subgroup. Moreover it is the smallest subgroups containing a.*

Proof. We begin by showing that H is a subgroup.

- We start by showing that $e \in H$. This is true since $a^0 = e \in H$ by definition.
- We now show that H is closed under the group operation. In fact, assume $b, c \in H$. Then we can write $b = a^n$ and $c = a^m$ by definition of H, so that $bc = a^n a^m = a^{n+m}$. Therefore $bc \in H$. Note that the fact that $a^n a^m = a^{n+m}$ ought to be proved by induction, as would the fact that $(a^n)^m = a^{nm}$.
- We now show that H is closed under taking inverses. Assume $b \in H$. As before, we write $b = a^n$ by definition of H. It follows that $b^{-1} = (a^n)^{-1} = a^{-n}$. Therefore $b^{-1} \in H$.

We now show that H is the smallest subgroup containing a. To do so we must show that any subgroup of G containing a must contain H. Assume H' is a subgroup of G containing a. Then by definition of subgroups H' contains all the positive powers of a, since it is closed under teh group operation. It also contains a^0 since $e \in H'$ by definition. Similarly it contains all the negative powers of a, since it is closed under inverses. Therefore $H \subset H'$. This proves the theorem. □

Definition 13.3. A group G is **cyclic** if $G = \langle a \rangle$ for some $a \in G$. We call such a the **generator** or G.

We see that this captures the motivating idea we introduced earlier.

Example 13.4. We showed that $\mathbb{Z}$ is cyclic: indeed $\mathbb{Z} = \langle 1 \rangle$. So 1 is a generator of $\mathbb{Z}$. However, 2 is not a generator, since $\langle 2 \rangle$ is the set of even integers. On the other hand, -1 is a generator.

Remark. In general

$$\langle a \rangle = \langle a^{-1} \rangle.$$

So a is a generator if and only if a^{-1} is a generator.

Example 13.5. The group $(\mathbb{Z}, +)$ is a cyclic group, and on of its generators is $[1]$. By the above remark we also have that $[-1] = [n-1]$ is a generator.

Example 13.6. Consider $n = 5$. In this case, there are generators other than $[1]$ and $[-1]$. We can check, for example, that $[3]$ is a generator. For instance, $[1]$ can be written as $[3] + [3] = [6] = [1]$. Since $[1]$ is a generator it follows that $[3]$ is also a generator. Similarly we can see that $[2]$ is a generator since $[1] = [2] + [2] + [2]$. Therefore, all nonzero elements of $\mathbb{Z}_n$ are generators.

Example 13.7. In the case of $n = 12$ we see that not all nonzero elements are generators. For example, $[2]$ is not a generator since it only generates even numbers. Its order is 6, since $[0] = [12] = [2] + [2] + [2] + [2] + [2] + [2]$. We can list the order of all the elements of $\mathbb{Z}_{12}$.

element	order	element	order
[0]	1	[1]	12
[2]	6	[3]	4
[4]	3	[5]	12
[6]	2	[7]	12
[8]	3	[9]	4
[10]	6	[11]	12

In particular we can prove that any time an element has the order the size of the group, then it is a generator. The book contains some formulae to compute the order of elements in a cyclic group. There are more patterns to this table; for example, primes always generate the group, and in general an element generates the group only if it is coprime to 12. This holds in the general case of $\mathbb{Z}_n$.

Example 13.8. The group D_3 is no cyclic. In fact, we see that all proper subgroups are cyclic, but there is no way to generate the whole group using one generator since every element generates a *proper* subgroup of D_3. Indeed we could have proved this using the following fact.

Theorem 13.9. *Any cyclic subgroup is abelian.*

Proof. Assume $G = \langle a \rangle$. Let $b, c \in G$. Then by definition $b = a^n$ and $c = a^m$. Therefore

$$bc = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = cb.$$

Therefore G is abelian. □

Theorem 13.10. *Any subgroup of a cyclic group is cyclic.*

Proof. Assume G is cyclic with generator a. Assume H is a subgroup of G. If $H = \{e\}$ then $H = \langle e \rangle$ and so it is cyclic. Assume now $H \neq \langle e \rangle$. Then there is $n \neq 0$ such that $a^n \in H$. If $n < 0$ then $(a^n)^{-1} \in H$ by taking inverses. So there is a strictly positive power of a in H. Let m be the minimal positive integer such that $a^m \in H$. We claim that $H = \langle a^m \rangle$.

- We first prove that $\langle a^m \rangle \subset H$. For $k \in \mathbb{Z}$ we know that $(a^m)^k \in H$ since $a^m \in H$ and H is a subgroup.
- We now prove that $H \subset \langle a^m \rangle$. Assume $x \in H$. Then $x = a^k$ for some $k \in \mathbb{Z}$. Let r be the remainder of the division of k by m, that is to say, $0 \leq r < m$ and $k = mq + r$ for some q. Therefore

  $$a^k = a^{mq+r} = (a^m)^q \cdot a^r.$$

  By assumption $(a^m) \in H$ and so $(a^m)^q \in H$ as H is a subgroup. It follows that $((a^m)^q)^{-1}$ and therefore

  $$\left((a^m)^q\right)^{-1} a^k = a^r \in H.$$

  So $a^r \in H$, and the only possibility is that $r = 0$ as m is minimal. This means that $x = (a^m)^q$, whic means that $x \in \langle a^m \rangle$. This finishes the proof.

□

14. Friday, October 26

14.1. **Cosets and Lagrange's theorem.** If you have a group, a very good way to understand it is to understand its subgroups. To this end, a powerful tool is Lagrange's theorem:

Theorem 14.1 (Lagrange)**.** *If H is a subgroup of G (with G finite), then the order of H divides the order of G.*

Example 14.2. An example of this is the subgroup $\langle[3]\rangle = \{[0],[3],[6],[9]\} \subset \mathbb{Z}_{12}$, whose order is 4 and divides 12. Another example is the rotation subgroup of D_3, which has order 3 and divides 6.

For the proof we are going to need the definition of cosets.

Definition 14.3. Assume G is a group and H is a subgroup of G. For $g \in G$, the **left coset of** H **with representative** g is

$$gH = \{gh | h \in H\}.$$

Analogously, the **right coset of** H **with representative** g is

$$Hg = \{hg | h \in H\}.$$

Note that $g \in gH$ always, since taking $h = e$ (which we can do since H is a subgroup) means that $g = gh$.

Example 14.4. Let $G = \mathbb{Z}_{12}$ amd $H = \langle[3]\rangle$. Some of the left cosets are

$$\begin{aligned}
[0]+H =&\{[0],[3],[6],[9]\}\\
[1]+H =&\{[1],[4],[7],[10]\}\\
[2]+H =&\{[2],[5],[8],[11]\}\\
[3]+H =&[0]+H = H\\
[4]+H =&[1]+H\\
[5]+H =&[2]+H\\
[9]+H =&[6]+H = [3]+H\\
[10]+H =&[7]+H = [4]+H\\
[11]+H =&[8]+H = [5]+H.
\end{aligned}$$

So H has three left cosets of G.

Student question: In this case, G is abelian. Does it follow that the right cosets are the same as the left cosets?

Answer: That is right. We are now going to see an example that involves a group which is not abelian.

Example 14.5. Let $G = D_3 = \{\mathrm{id}, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$ and $H = \{\mathrm{id}, \mu_1\}$. Then some of the left cosets are

$$\begin{aligned}
\mathrm{id} \circ H =&\{\mathrm{id}, \mu_1\} = H\\
\rho_1 \circ H =&\{\rho_1, \mu_3\}\\
\rho_2 \circ H =&\{\rho_2, \mu_2\}.
\end{aligned}$$

The other cosets are given by the one above; in fact we can check that

$$\begin{aligned}\mu_1 \circ H =& \mathrm{id} \circ H\\ \mu_3 \circ H =& \rho_1 \circ H\\ \mu_2 \circ H =& \rho_2 \circ H.\end{aligned}$$

Thus there are three left cosets. How about the right cosets? We have that

$$\begin{aligned}H \circ \mu_1 = H \circ \mathrm{id} =& \{\mathrm{id}, \mu_1\}\\ H \circ \mu_2 = H \circ \rho_1 =& \{\rho_1, \mu_2\}\\ H \circ \mu_3 = H \circ \rho_2 =& \{\rho_2, \mu_3\}.\end{aligned}$$

Thus there are three right cosets, and they are different from the left cosets.

In assignment 12 problem 6 we had a group G and a subgroup H. We defined an equivalence relation on G by $a \sim b$ if $a = bh$ for some $h \in H$. How does this equivalencee relation relate to cosets?

Example 14.6. Let $G = \mathbb{Z}_6$ and $H = \{[0],[3]\}$. In this case, the equivalence classes are

$$\begin{aligned}[0] + H &= \{[0],[3]\}\\ [1] + H &= \{[1],[4]\}\\ [2] + H &= \{[2],[5]\}\end{aligned}$$

and so we see that the left cosets and equivalence classes are the same in this case.

It turns out that the result of the previous example holds in general.

Theorem 14.7. *The equivalence classes of $\sim$ are the same as the left cosets. More precisely, for $a \in G$,*

$$aG = \{b \in G | a \sim b\} = [a].$$

Proof. We start by proving that

$$aH \subset \{b \in G | a \sim b\}.$$

Assume $x \in aH$. This means that $x = ah$ for some $h \in H$. So $a \sim x$ by definition of $\sim$. Therefore $x \in \{b \in G | a \sim b\}$.

We now prove that

$$\{b \in G | a \sim b\} \subset aH.$$

Assume $x \in \{b \in G | a \sim b\}$. Then $a \sim x$. So $a = xh$ for some $h \in H$. This means that $ah^{-1} = x$. We know that H is a subgroup, and thus $h^{-1} \in H$. Let $h' = h^{-1}$. Then $x = ah'$ for some $h' \in H$. Therefore $x \in aH$.

In conclusion, left cosets are equivalence classes of $\sim$. □

Consequence. The left cosets form a partition.

Proof. We proved that any equivalence relation will induce a partition given by its equivalence classes. □

In particular, left cosets are disjoint and cover all of G.

Example 14.8. Consider $G = \mathbb{Z}$ and H being the subgroup of even numbers. Then the corresponding equivalence relation is congruence mod 2. In particular

$$0 + H = \{0, 2, -2, 4, \dots\} = [0]$$
$$1 + H = \{1, -1, 3, \dots\} = [1].$$

If G is finite, and $g_1H, g_2H, \dots, g_kH$ are the cosets, we see that

$$|G| = |g_1H| + \cdots + |g_kH|$$

since the cosets form a partition. It turns out that $|gH| = |H|$for all $g \in G$, which allows us to simplify the above expression.

Theorem 14.9. *Assume G is finiteand H is a subgroup. Then any left coset has the same cardinality.*

Proof. Assume $g \in G$. We give a bijection $f : H \to gH$. Define $f(h) = gh$. This is well defined since elements of gH are of the form gH.

We now prove f is an injection. Assume $h_1, h_2 \in H$ and $f(h_1) = f(h_2)$. So $gh_1 = gh_2$, and therefore $h_1 = h_2$.

We now prove f is a surjection. Assume $y \in gH$. So $y = gh$ for some $h \in H$. This means that $y = f(h)$, and f is surjective. □

Definition 14.10. Assume H is a subgroup of G. The **index** of H in G, written $[G : H]$, is the number of left cosets of H in G.

From this it follows that

Theorem 14.11 (Lagrange)**.** *For a finite group G with H a subgroup we have that*

$$|G| = [G : H] \cdot |H|.$$

In particular, $|H|$ divides $|G|$.

Proof. Since left cosets form a partition of G, we know that

$$|G| = |g_1H| + \cdots + |g_kH|$$

where $k = [G : H]$. Since every coset has cardinality $|H|$, it follows that

$$|g_1H| + \cdots + |g_kH| = [G : H] \cdot |H|$$

and so

$$|G| = [G : H] \cdot |H|$$

□

Corollary 14.11.1. *Assume G is finite. Then the order of any $a \in G$ divides $|G|$.*

Proof. Assume $H = \langle a \rangle$. By Lagrange's theorem, $|H|$ divides $|G|$. But we know that $|\langle a \rangle|$ is equal to the order of a, and so the order of a divides $|G|$. □

Corollary 14.11.2. *Assume p is a prime, and assume G is a group with p elements. Then any element of G except the identity has order p. So $\langle a \rangle = G$ for all $a \neq e$ and therefore G is cyclic. In particular $G \cong \mathbb{Z}_p$.*

15. Monday, October 29

15.1. **Quotient groups (or: modular arithmetic generalized).** Let's review the definiton of $(\mathbb{Z}_n, +)$, say with $n = 5$. We start with the group $(\mathbb{Z}, +)$. For $a, b \in \mathbb{Z}$ we define $a \equiv_5 b$ if 5 divides $a - b$ (that is to say, $a - b = 5k$ for some $k \in \mathbb{Z}$). This is an equivalence relation; in particular we define $\mathbb{Z}_5$ to be the set of all equivalence classes of $\equiv_5$. In this case, we can write

$$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}.$$

Then we defined an operation on these equivalence classes, defined by

$$[a] + [b] = [a + b].$$

To check that this is a well defined function we need to check that if $a \equiv_5 c$ and $b \equiv_5 d$ (that is, $[a] = [c]$ and $[b] = [d]$) then $a + b \equiv_5 c + d$ (i.e. $[a + b] = [c + d]$). We can check that this is the case, and therefore $(\mathbb{Z}_n, +)$.

Note that this is a special property, and it does not follow for all operations. For example, the operation $[a]^{[b]} = [a^b]$ is not well-defined, since we can take $[a] = 4, [b] = 2$ and $[c] = -1, [d] = 7$ and we see that while $[a] = [c], [b] = [d]$, the result is not independent on the choice of representative:

$$a^b \equiv_5 1 \not\equiv_5 c^d = -1.$$

We now want to generalize this construction. The first step is going to be the same, i.e. we are going to start with a group G. For the second step, we see that the integer case can be reformulated as saying that $a \equiv_5 b$ if $a - b$ lies in the subgroup of multiples of 5. Thus, we might want to formulate our generalized construction based on cosets, seeing as they too involve this kind of equivalence relation. Let's see this in detail.

Assume $(G, *_G)$ is a group, and let H be a subgroup. We can define an equivalence class on G by letting $a \sim b$ if $a = bh$ for some $h \in H$. Last time we saw that the equivalence classes of this relation are precisely the left cosets $g * H = \{g * h | h \in H\}$. (As seen in 14.8, the cosets in our particular example are $[0] = 0 + H, [1] = 1 + H$, and so on). We would now like to define a group G/H whose set will be the left cosets. For the operation, we want it to be defined as

$$(g_1 * H) * (g_2 * H) = (g_1 * g_2) * H.$$

This is precisely what we did with $(\mathbb{Z}, +)$; however, we will see that it doesn't always work. The following theorem indicates when it does work.

Theorem 15.1. *Assume H is a* ***normal subgroup*** *of G (that is, $gH = Hg$ for all $g \in H$). Then for any $a, b, c, d \in G$ such that $aH = cH$ and $bH = dH$ then $(ab)H = (cd)H$.*

Notation. For any subset A of G and $g \in G$ we define

$$gA = \{ga | a \in A\} \quad Ag = \{ag | a \in A\}.$$

Note that $(gA)g' = g(Ag')$ and $g(g'A) = (gg')A$ for any $g, g' \in G$. This is almost the definition of cosets, with the difference that A need not be a subgroup.

Proof. By using the notation we just introduced, we can write $(ab)H = a(bH)$, and in turn we know that $a(bH) = a(dH)$ by assumption. Since H is a subgroup we know that $a(dH) = a(Hd)$. Similarly,

$$a(Hd) =(aH)d = (cH)d = c(Hd) = c(dH) = (cd)H.$$

Thus $(ab)H = (cd)H$. □

Definition 15.2. Assume G is a group, and assume that N is a normal subgroup of G. We define the **quotient group** G/N (also known as **factor group**) as follows: G/N is the set of (left) cosets of N in G. The operation is defined by $(aN)(bN) = (ab)N$.

By the last theorem the operation is well-defined. We claim that G/N is a group.

Proof. We start by checking the operation is associative. In fact, we see that

$$aH(bHcH) = a(bc)H = (ab)cH = (aHbH)cH$$

by associativity of the original group operation on G.

The identity of the group is $eH = H$ since

$$gHeH = geH = gH$$

by definition.

Given $gH \in G/H$ we claim that the inverse is $(gH)^{-1} = g^{-1}H$. In fact,

$$gHg^{-1}H = gg^{-1}H = eH.$$

□

Intuitively, we can think of G/N as G but with all the elements of N identified.

Example 15.3. Consider the symmetries of an equilateral triangle $(D_3, \circ)$ with elements $\{\mathrm{id}, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$. We consider now the subgroup $N = \{\mathrm{id}, \rho_1, \rho_2\}$. It turns out that this is a normal subgroup. By Lagrange's theorem, there are 2 cosets in the set G/N (since $|G/N| = |G|/|N|$). Specifically we find that

$$G/N = \{\{\mathrm{id}, \rho_1, \rho_2\}, \{\mu_1, \mu_2, \mu_3\}\},$$

namely the cosets are the rotations and the reflections. Since the second coset squared is equal to the identity (for example, $\mu_1 N \mu_1 N = \mu_1^2 N = N$) we see that G/N is actually isomorphic to $\mathbb{Z}/2$.

Example 15.4. If we consider $N = G$ then $G/N = \{G\}$, i.e. the quotient group is a group with one element. If $N = \{e\}$ then the cosets are given by $gN = \{g\}$. Thus

$$G/N = \{\{g\} | g \in G\}.$$

This is isomorphic to G with isomorphism $f : G/N \to G$ given by $f(\{g\}) = g$.

Example 15.5. We can consider $G = (\mathbb{R}, +)$ and $N = \mathbb{Z}$. In this case, G/N can be seen as a circle, seeing as $[1]$ and $[0]$ are identified.

16. Friday, November 2

16.1. **Quotient groups: the first isoorphism theorem.** Recall that given a group G and a *normal subgroup* N we defined the quotient group $(G/N, *)$ as the set of cosets of N (i.e. $\{G/N = \{gN | g \in G\}\}$) such that $g_1Ng_2N \overset{\text{def}}{=} (g_1g_2)N$. This is a group with identity $eN = N$ and inverses $(gN)^{-1} = g^{-1}N$.

Example 16.1. As we saw last time, we have that $\mathbb{Z}/5\mathbb{Z}$ (where $5\mathbb{Z}$ is shorthand for multiples of 5) is the same thing as $\mathbb{Z}_5$. Another example is $D_3/\langle r\rangle$ (where r is a rotation) which is equal to

$$D_3/\langle r\rangle = \{\text{id}\langle r\rangle, s\langle r\rangle\}$$

where s is some reflection. We see that the multiplication table of this group is

	$\text{id}\langle r\rangle$	$s\langle r\rangle$
$\text{id}\langle r\rangle$	$\text{id}\langle r\rangle$	$s\langle r\rangle$
$s\langle r\rangle$	$s\langle r\rangle$	$\text{id}\langle r\rangle$

and we see that it is isomorphic to $\mathbb{Z}_2$ via the isomorphism $[0] \to \text{id}\langle r\rangle$ and $[1] \to s\langle r\rangle$. We could also deduce that it is isomorphic to $\mathbb{Z}_2$ just looking at the number of elements. In fact, if a group G has p elements, where p is prime, we know it must be cyclic. This follows from Lagrange's theorem: take $a \in G$ such that $a \neq e$, and consider the subgroup $H = \langle a\rangle$. By Lagrange's theorem, $|H|$ divides p. Since $e, a \in H$ we know that $|H| \geq 2$, and so $|H| = p$. It follows that $G = H$ and G is cyclic.

Today we are going to talk about quotient groups and homomorphisms.

Remark. Given a group G and a normal subgroup N of G, there is a homomorphism

$$f : G \to G/N$$

given by $f(g) = gN$. Such f is called the **canonical homomorphism**.

Example 16.2. Let $G = \mathbb{Z}$ and $N = 5\mathbb{Z}$ (the multiples of 5) so that $G/N = \mathbb{Z}/5$. In this case

$$f(n) = n + 5\mathbb{Z}.$$

In particular,

$$\begin{aligned} f(0) &= \{0, -5, 5, 10, -10, \dots\} \\ f(1) &= \{1, 6, -4, \dots\} \\ &\vdots \\ f(n) &= [n]_{\text{mod } 5}. \end{aligned}$$

Note: The map f (in the general case) is indeed a homomorphism: assume $g_1, g_2 \in G$. Then

$$f(g_1g_2) = (g_1g_2)N = g_1Ng_2N = f(g_1)f(g_2).$$

What is $\ker(f)$? Recall that by definition

$$\ker(f) = \{g \in G | f(g) = eN = N\}.$$

So it follows that

$$\begin{aligned}&\{g \in G | f(g) = eN = N\}\\=&\{g \in G | gN = N\}.\end{aligned}$$

We claim that this set is equal to N. We prove this by proving both inclusions of sets.

We start by proving that $N \subset \{g \in G | gN = N\}$. Assume that $n \in N$. Then $nN = N$, so that $n \in \{g \in G | gN = N\}$.

We now prove the reverse inclusion. Suppose $g \in G$ and $gN = N$. This means in particular that $ge \in N$. But $ge = g$ and so $g \in N$.

How about $\mathrm{im}(f)$? We claim that $\mathrm{im}(f) = G/N$, i.e. f is a surjection. In fact, given $x \in G/N$ we know that x is of the form gN for some $g \in G$. Therefore $x = f(g)$.

The conclusion is that

$$G/\ker(f) = \mathrm{im}(f) = G/N.$$

We are now going to develop a similar result in a more general setting. Assume $f : G \to H$ is a homomorphism. In assignment 14 you are going to prove the following theorem:

Theorem 16.3. *The subgroup* $\ker(f)$ *is a* normal *subgroup of* G*.*

The main result of today will be the following:

Theorem 16.4 (First isomorphism theorem)**.** *For a group homomorphism* $f : G \to H$ *we have that*

$$G/\ker(f) \cong \mathrm{im}(f).$$

A particular case of this is that $\ker(f) = \{e\}$ if and only if f is injective. In fact, if $\ker(f) = \{e\}$ then we saw last time that $G/\{e\} \cong G$, and therefore $G \cong G/\ker(f) \cong \mathrm{im}(f)$. On the other hand, if f is injective then f is an isomorphism from G to $\mathrm{im}(f)$.

16.1.1. *Proof of the first isomorphism theorem.* Write $K = \ker(f)$ and define $\bar{f} : G/K \to \mathrm{im}(f)$ by $\bar{f}(gK) = f(g)$. Since this definition involves a choice of representative, we need to prove it is well-defined: assume $g_1K = g_2K$. This means that we can write $g_1 = g_2k$ for some $k \in K$. Then

$$\begin{aligned}\bar{f}(g_1K) =& f(g_1)\\=&f(g_2k)\\=&f(g_2)f(k)\\=&f(g_2)e\\=&f(g_2)\\=&\bar{f}(g_2K).\end{aligned}$$

Having proved it's well-defined, we now prove that $\bar{f}$ is a homomorphism. Assume $g_1K, g_2K \in G/K$. Then

$$\bar{f}(g_1Kg_2K) =\bar{f}(g_1g_2K) = f(g_1g_2) = f(g_1)f(g_2) = \bar{f}(g_1K)\bar{f}(g_2K).$$

Proving that f is a bijection is not hard, so we will skip it (details can be found in the book). $\square$

Application. Assume G is a cyclic group of order n. Say $G = \langle a \rangle$ for some $a \in G$. Define a homomorphism $\mathbb{Z} \to G$ by $f(m) = a^m$. By the first isomorphism theorem we know that

$$\mathbb{Z}/\ker(f) \cong \operatorname{im}(f) = G.$$

But we see that

$$\begin{aligned}\ker(f) =& \{m \in \mathbb{Z} | a^m = e\}\\ =& \{\text{ multiples of } n\}\\ =& n\mathbb{Z}\end{aligned}$$

and therefore $\mathbb{Z}/n\mathbb{Z} \cong G$.

17. Monday, November 5

17.1. Topology of the real line. [1]

The real line is the set of real numbers. The real numbers have some properties that distinguish them from other setss of numbers such as the rationals. For example, the rationals don't contain a lot of numbers that the reals might contain. But what it means for a number to be a real number? To answer to this question we are first going to list some *axioms* (i.e. exactly what we are assuming about $\mathbb{R}$).

17.2. Axioms of the real numbers.

There is:

- a set $\mathbb{R}$;
- binary operations $+$ and $\cdot$ on $\mathbb{R}$;
- a relation $<$ on $\mathbb{R}$;

satisfying:

(A) $(\mathbb{R},+)$ is an abelian group with identity denoted by 0;
(M) $(\mathbb{R}-\{0\},\cdot)$ is an abelian group with identity denoted by 1; also, $\cdot$ is commutative and associative on all of $\mathbb{R}$;
(D) for all reals x,y,z we have that

$$x(y+z)=(xy)+(xz);$$

(O) the relation $<$ satisfies:
  (O1) trichotomy: for all reals x, exactly one of $0<x$, $x=0$, or $x<0$ is true;
  (O2) for all $x,y\in\mathbb{R}$ if $0<x$ and $0<y$ then $0<x+y$ and $0<x\cdot y$;
  (O3) for all $x,y,z\in\mathbb{R}$ if $x<y$ then $x+z<y+z$.
(C) completeness axiom: we will discuss this on Friday.

Axiom (C) is necessary to distinguish real numbers from the rationals, since the latter satisfy all of the other axioms.

We also introduce the following definitions:

Definition 17.1. We define $x>y$ to mean $y<x$.

Definition 17.2. We define $x-y\in\mathbb{R}$ as $x-y=x+(-y)$.

Definition 17.3. We define $x/y\in\mathbb{R}$ as $x/y=x\cdot(y^{-1})$ and write xy for $x\cdot y$.

We now move onto some facts.

Facts.

(F0) We have that $x\cdot 0=0$;
(F1) we have that $-(xy)=(-x)y$.

Some of these facts are going to be part of your homework; for now, let's prove that $x\cdot 0=0$.

Proof. From (A) we know that $0=0+0$. So

$$\begin{aligned} x\cdot 0 &= x\cdot(0+0)\\ &\overset{(D)}{=}(x\cdot 0)+(x\cdot 0). \end{aligned}$$

[1] Handout at `http://www.math.harvard.edu/~sebv/101-fall-2018/reals.pdf`

So

$$0 = x \cdot 0 + (-x \cdot 0) = x \cdot 0 + \cdot 0 + (-x \cdot 0) = x \cdot 0.$$

□

We also have the following fact:

Fact. For every $y \geq 0$ there is a unique $x \geq 0$ such that $x^2 = y$.

This fact is not true for rational numbers, so we will be using axiom (C) to prove existence; we will do this on Friday. However, we are able to prove uniqueness, namely prove that given $x_1, x_2 \geq 0$ then $x_1^2 = x_2^2$ only if $x_1 = x_2$.

The above fact allows us to introduce the following definition:

Definition 17.4. For $y \geq 0$ we define $\sqrt{y}$ to be the unique $x \geq 0$ such that $x^2 = y$.

Definition 17.5. For x a real number, we define

$$|x| = \begin{cases} x & x \geq 0 \\ -x & \text{otherwise.} \end{cases}$$

Some basic properties of the absolute value are as follows:

- For $x, y \in \mathbb{R}$ we have that $|xy| = |x||y|$;
- $x \leq |x|$;
- $|x| \geq 0$ and $|x| > 0$ if $x \not 0$;
- $|x|^2 = |x^2|$;
- $|x|\sqrt{x^2}$.

One of the most important facts about the absolute value is the following:

Theorem 17.6 (Triangle inequality (1.2.5 in the handout))**.** *For real numbers $x, y \in \mathbb{R}$ we have that*

$$|x + y| \leq |x| + |y|.$$

An important consequence is the following: assume $z \in \mathbb{R}$. Then $|x - y| \leq |x - z| + |z - y|$. If we imagine x, y, z being vertices of a triangle then this fact tells us that going straight from x to y takes less than going from x to z first and then from z to y. This is what this this inequality its name. T he proof of this fact (given the triangle inequality) is the following:

$$\begin{aligned} |x - y| &= |x - z + z - y| \\ &\leq |x - z| + |z - y|. \end{aligned}$$

We are now going to introduce a theorem that will be a useful tool to prove that two real numbers are equal.

Theorem 17.7. *For $x, y \in \mathbb{R}$ we have that $x = y$ if and only if $|x - y| < \varepsilon$ for every $\varepsilon > 0$.*

Proof. Assume $x, y, \varepsilon \in \mathbb{R}$ with $\varepsilon > 0$, and assume $x = y$. Then

$$|x - y| = |x + (-y)| = |x + (-x)| = |0| = 0 < \varepsilon.$$

This proves the “only if” direction.

Assume now $|x-y| < \varepsilon$ for every $\varepsilon > 0$. Assume for a contradiction that $x \neq y$. Write $z = x - y$. We know that $z \neq 0$, and therefore $|z| > 0$ (this is one of the basic properties listed above). Write $\varepsilon_0 = |z|$. Then by assumption

$$\varepsilon_0 = |z| = |x-y| < \varepsilon_0,$$

so $\varepsilon_0 < \varepsilon_0$, which is a contradiction by (F6) in the handout. □

18. Friday, November 9

18.1. **The completeness axiom of the real numbers.** Last time we introduced the axioms of the real numbers, and we noted that there is an axiom that makes the real number different from the rationals. This axiom is called the **axiom of completeness**:
Axiom of completeness. Any non-empty set of real numbers that is bounded above has a least upper bound.

Definition 18.1. A set A of real numbers is **bounded above** if there is $b \in \mathbb{R}$ such that $a \le b$ for all $a \in A$. We call b and **upper bound** for A. Similarly define **bounded below** and **lower bound** by replacing $\le$ by $\ge$ in the above definition.

Example 18.2. The interval $A = (0,1)$ is bounded above, for example by 1. Note that you don't have to consider 1 as the only upper bound; any number $x \ge 1$ will work.

Example 18.3. The interval $A = (0,\infty)$ is not bounded above, but it is bounded below. Note that in our notation ∞ is not a real number.

Definition 18.4. Given a non-empty set A of real numbers, a real number $b \in \mathbb{R}$ is a **least upper bound** (or **supremum**) of A if

(1) b is an upper bound;
(2) for any upper bound s of A we have that $b \le s$.

If b is the least upper bound of A we write $b = \sup(A)$.

Note that the least upper bound is unique. In fact, if b_1 and b_2 are least upper bounds of A, then by (1) b_1 is an upper bound and so by (2) we know that $b_2 \le b_1$. Similarly $b_1 \le b_2$.

Example 18.5. We claim that if $A = (0,1)$ then $\sup(A) = 1$.

Proof. We chekc that b satisfies the definition of least upper bound.

(1) We claim that 1 is an upper bound of $(0,1)$. In fact, assume $a \in (0,1)$. Then by definition of $(0,1)$ it follows that $a < 1$, so $a \le 1$.
(2) Assume s is any upper bound of $(0,1)$. Assume for a contradiction that $s < 1$. Then $s \in (0,1)$ or $s \le 0$. We now want to show that there is something strictly bigger than s which is less than 1. Consider $a = (s+1)/2$. We can prove using the axioms that $s < a < 1$. Then a shows that s is not an upper bound.

□

Warning. The least upper bound is not the same as the maximum.

Definition 18.6. A **maximum** of A is an element $a_0 \in A$ such that $a \le a_0$ for all $a \in A$.

Example 18.7. The set $(0,1)$ has no maximum but it has a supremum; on the other hand, the set $(0,1]$ has a maximum (and a supremmum). In particular, if s is a maximum then it is a supremum, but not vice versa.

Example 18.8. Consider $A = \left\{ r \in \mathbb{Q} \,|\, r^2 \le 2 \right\}$. It looks like $\sup(A) = 1$, which we need to prove. Note that this set does not have a supremum in $\mathbb{Q}$; in fact, we are going to prove that if $a < b$ are real numbers then there is a rational r such that $a < r < b$. This property of the rationals is summarized by saying that the rationals are **dense** in $\mathbb{R}$.

18.2. **Nested interval property.** Consider a collection of intervals $[a_1, b_1], [a_2, b_2], \ldots$ that are nested. Then the next theorem shows that the properties of the real numbers are going to imply that there is some number in the intersection.

Theorem 18.9. *Assume for each $n \in \mathbb{N}$ we are given a non-empty closed interval $I_n = [a_n, b_n]$. Assume $I_{n+1} \subset I_n$ for all $n \in \mathbb{N}$. Then*

$$\bigcap_{n \in \mathbb{N}} I_n \neq \emptyset.$$

Remark. Note that it is crucial that the intervals here are closed. For a counterexample where they are not closed, consider

$$\bigcap_{x>0} (0, x) = \emptyset.$$

Proof. Let

$$A = \{x \in \mathbb{R} | x \leq b_n \text{ for all } n \in \mathbb{N}\}.$$

We claim that A is bounded above. In fact, b_n is an upper bound for all $n \in \mathbb{N}$. Moreover, A is not empty, since $a_n \in A$ for all $n \in \mathbb{N}$. By the completeness axiom it follows that $y = \sup(A)$ exists. We now want to prove that $y \in \cap_{n \in \mathbb{N}} I_n$. To do so we need to prove that $y \in I_n$ for all $n \in \mathbb{N}$. Assume $n \in \mathbb{N}$. Then $y \leq b_n$, because b_n is an upper bound and y is the *least* upper bound, and so by definition $y \leq b_n$. Also $a_n \leq y$ since $a_n \in A$ and y is an upper bound of A by definition of least upper bound. Therefore $y \in I_n$, and so

$$y \in \bigcap_{n \in \mathbb{N}} I_n.$$

□

Studen question: how is this result logically related to the completeness axiom?
Answer: it turns out that the two are actually equivalent statements.

18.3. **The archimedean property.** The archimedean property of the real numbers states that

(i) for all $x \in \mathbb{R}$, there is $n \in \mathbb{N}$ such that $x \leq n$;
(ii) for all $x > 0$ there is $n \in \mathbb{N}$ such that $1/n < x$.

Proof. We start by proving (i). Assume for a contradiction that there exists $x \in \mathbb{R}$ such that $n < x$ for all $n \in \mathbb{N}$. Take $A = \mathbb{N}$. By our assumption, A is bounded above by x. Therefore we can take $\alpha = \sup(A)$. Consider now $\alpha - 1$. We know that $\alpha - 1$ is not an upper bound for $\mathbb{N}$. This means that there is $n \in \mathbb{N}$ with $\alpha - 1 < n$. Then $\alpha < n + 1$, and since $n + 1 \in \mathbb{N}$ it follows that α is not an upper bound. This contradicts our assumption that $\alpha = \sup(\mathbb{N})$.

We now prove (ii), and we will use part (i) to do this. Assume $x > 0$ and take $y = 1/x$. Apply (i) to y to get $n \in \mathbb{N}$ with $y \in n$. So $y < n + 1$. Then

$$x = \frac{1}{y} > \frac{1}{n+1}.$$

□

Corollary 18.9.1. *For any $a, b \in \mathbb{R}$ with $a < b$ there is a rational number r with $a < r < b$.*

For a proof of this, see the book; what we just did is the special case $a = 0$.

Theorem 18.10. *There is $\alpha \in \mathbb{R}$ such that $\alpha^2 = 2$.*

Proof. Let

$$A = \left\{ x \in \mathbb{R} \,|\, x^2 \leq 2 \right\}.$$

This is nonempty since $0 \in A$, and A is bounded above by 2. Let $\alpha = \sup(A)$. We claim that $\alpha^2 = 2$.

Proof of claim. Assume that $\alpha^2 \neq 2$. If $\alpha^2 < 2$ then $\alpha \in A$. We will find $\beta \in A$ such that $\alpha < \beta$. For $n \in \mathbb{N}$ we have that

$$\begin{aligned} \left(\alpha + \frac{1}{n} \right) =& \alpha^2 + \frac{2\alpha}{n} + \frac{1}{n^2} \\ \leq& \alpha^2 + \frac{2\alpha}{n} + \frac{1}{n} \\ =& \alpha^2 + \frac{2\alpha + 1}{n}. \end{aligned}$$

So $\alpha^2 + (2\alpha + 1)/n < 2$ if $(2\alpha + 1)/n < 2 - \alpha^2$. Such n exists by the archimedean property. □

□

19. Monday, November 12

19.1. **Limits of sequences.**

Last time we saw that

$$\sqrt{2} = \sup\Big(\Big\{x \in \mathbb{R} | x^2 < 2\Big\}\Big).$$

Intuitively, we can think of this as saying that if we look at the real line and we consider all the points such that $x^2 < 2$, then they are bounded on the left by $x = \sqrt{2}$. Another way of looking at it is to consider $\sqrt{2}$ as the limit of the sequence $1, 1.4, 1.41, \ldots$. Today we will see how to make this last concept precise.

Definition 19.1. A **sequence** is a function whose domain is $\mathbb{N}$.

Example 19.2. Let $f : \mathbb{N} \to \mathbb{R}$ be defined as $f(n) = 1/n$. This is the sequence

$$1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots.$$

Notations. In practice we never write out sequences as functions. Rather we use the following notations:

- $(a_1, a_2, a_3, \ldots)$, which in the previous example would be $\left(1, \frac{1}{2}, \frac{1}{3}, \ldots\right)$;
- $(a_n)_{n\in\mathbb{N}}$, which in the previous example would be $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$;
- $(a_n)_{n=1}^{\infty}$ $(\big(\frac{1}{n}{}_1^{\infty}\big)$ in the example);
- (a_n) $(\big(\frac{1}{n}\big)$ in the example).

Definition 19.3. A sequence (a_n) **converges** to a real number a if for every $\varepsilon > 0$ there exists a natural number N such that whenevr $n \geq N$ we have $|a_n - a| < \varepsilon$. If it exists, the number a is called the **limit** of the sequence (a_n), and is written as $\lim_{n\to\infty}(a_n) = a$ or $(a_n) \to a$.

Example 19.4. Consider the sequence (a_n) given by $a_n = \frac{1}{\sqrt{n}}$. Then you might know from calculus that $(a_n) \to 0 = a$. We now want to prove this rigorously. We have to check that for every $\varepsilon > 0$ there is N such that whenever $n \geq N$ then

$$\left|\frac{1}{\sqrt{n}} = 0\right| = \left|\frac{1}{\sqrt{n}}\right| < \varepsilon.$$

For example, given $\varepsilon = 1/10$ we see that $N = 101$ works, since $\frac{1}{\sqrt{101}} < \frac{1}{\sqrt{100}} = 1/10 = \varepsilon$; similarly for $\varepsilon = 1/100$ we see that $N = 10001$ works. We want to show this in the general case. The template is as follows: Assume $\varepsilon > 0$. Take N such that … (or $N = \ldots$). We now show it works. Assume $n \geq N$.

$$\vdots$$

Therefore $|a_n - a| < \varepsilon$.

How can we use this template in our case where $a_n = \frac{1}{\sqrt{n}}$? We see that we need to check that

$$\left|\frac{1}{\sqrt{n}} = 0\right| = \left|\frac{1}{\sqrt{n}}\right| < \varepsilon,$$

, and if we square both sides we get

$$\frac{1}{n} < \varepsilon^2.$$

Let's put this into our proof.

Proof. Assume $\varepsilon > 0$. Take N such that

$$\left(\frac{1}{\varepsilon}\right)^2 < N.$$

Such N exists by the archimedean property of the natural numbers. We now show it works. Assume $n \geq N$. Since $(1/\varepsilon)^2 < N$ it follows that $\frac{1}{\varepsilon} < \sqrt{N}$, and therefore $1/\varepsilon < \sqrt{n}$ since $\sqrt{N} \leq \sqrt{n}$. Therefore

$$|a_n - a| \leq \varepsilon.$$

□

Example 19.5. Consider (a_n) where $a_n = \frac{n+1}{n}$. We want to prove that $(a_n) \to 1$.

Proof. Assume $\varepsilon > 0$. Take a natural number N such that $1/N < \varepsilon$ (this exists by the Archimedean property). We now show it works. Take a natural number $n \geq N$. Then

$$|a_n - a| = \left|\frac{n+1}{n} - 1\right| = \left|\frac{1}{n}\right| = \frac{1}{n} \leq \frac{1}{N} < \varepsilon,$$

as desired. □

We are going to introduce some facts that are going to be useful when computing limits. The first is the **algebraic limit theorem**, and the second is the **order limit theorem**.

Theorem 19.6 (Algebraic limit theorem). *Assume $(a_n) \to a$ and $(b_n) \to b$. Then*

(i) $(ca_n) \to ca$ *for every real number* c;

(ii) $(a_n + b_n) \to a + b$;

(iii) $(a_n \cdot b_n) \to ab$;

(iv) $\left(\frac{a_n}{b_n}\right) \to \frac{a}{b}$ *if* $b_n \neq 0$ *for all* $n \in \mathbb{N}$ *and* $b \neq 0$.

Theorem 19.7 (Order limit theorem). *Assume $(a_n) \to a$ and $(b_n) \to b$. If $a_n \leq b_n$ for all natural numbers n, then $a \leq b$.*

We are not going to prove the Algebraic limit theorem in full, but rather we will limit ourselves to proving part (i). We will come back to the remaining parts once we develop tools to prove them efficiently.

Proof of (i) in the algebraic limit theorem. Assume c is a real number. Either $c = 0$ or $c \neq 0$. We can consider these two cases separately.

If $c = 0$ then $(ca_n) = (0) \to 0 = ca$.

Suppose now $n \neq 0$. We know that $(a_n) \to a$. So for every $\varepsilon_2 > 0$ there is $N \in \mathbb{N}$ such that whenever $n \geq N$ we have $|a_n - a| < \varepsilon$. We want to show that $(ca_n) \to ca$. Assume $\varepsilon > 0$. Set $\varepsilon_2 = \varepsilon/|c|$. By assumption, there is $N \in \mathbb{N}$ such that $|a_n - a| < \varepsilon_2$ whenever $n \geq N$. Assume that $n \geq N$. Then

$$|ca_n - ca| = |c||a_n - a| < |c|\varepsilon_2 = |c|\frac{\varepsilon}{|c|} = \varepsilon,$$

as desired. □

Proof of the order limit theorem. Assume $(a_n) \to a$ and $(b_n) \to b$. Assume $a_n \leq b_n$ for all n. Assume for a contradiction that $b < a$. Take $\varepsilon = \frac{a-b}{2}$. Then $\varepsilon > 0$ by assumption. Since $(a_n) \to a$ there is N_1 such that whenever $n \geq N_1$ we have $|a_n - a| < \varepsilon$. Since $(b_n) \to b$ there is N_2 such that whenever $n \geq N_2$ we have $|b_n - b| < \varepsilon$. Take $N = \max(N_1, N_2)$ and assume $n \geq N$. Then $|b_n - b| < \varepsilon$. So

$$b - \varepsilon < b_n < b + \varepsilon = b + \frac{a-b}{2} = \frac{a}{2} + \frac{b}{2}.$$

Similarly $|a_n - a| < \varepsilon$ and so

$$\frac{a}{2} + \frac{b}{2} = a - \frac{a-b}{2} = a - \varepsilon < a_n < a + \varepsilon.$$

So

$$b_n < b + \varepsilon = \frac{a}{2} + \frac{b}{2} = a - \varepsilon < a_n,$$

and so $b_n < a_n$. This contradicts our assumption that $a_n \leq b_n$. □

20. Friday, November 16

20.1. **Subsequences and limits.** Last time we saw what it means for a sequence (a_n) to converge to a real number a (written $(a_n) \to a$) if for every $\varepsilon > 0$ there exists a natural number N such that whenevr $n \geq N$ we have $|a_n - a| < \varepsilon$. If (a_n) does not converge we say it **diverges**. Today we will explore some conditions under which a sequence converges or diverges.

Definition 20.1. A sequence (a_n) is **bounded** if there exists a positive real number M such that $a_n \leq M$.

If we picture the sequence as dots on the real line, then it is bounded if there is an interval $[-M, M]$ that contains all the dots.

Example 20.2. The sequence $(01, 1, -1/2, 1/2, -1/3, \dots)$ is bounded: take $M = 1$. However, the sequence $(1, 2, 3, \dots)$ is not bounded, and the same goes for $(-1, -2, -3, \dots)$.

The following theorem gives us a useful necessary condition for convergence.

Theorem 20.3. *If a sequence (a_n) converges, then (a_n) is bounded.*

Proof. Assume (a_n) converges to a. Take $\varepsilon = 1$. Then there is $N \in \mathbb{N}$ such that whenever $n \geq N$ we have $|a_n - a| < 1$. Take $M = \max(|a_1|, |a_2|, \dots, |a_N|, |a+1|)$. Then for any n we have that $|a_n| \leq M$. □

Is the converse true? Namely, if a sequence (a_n) is bounded, then does it converge? The answer is no: for example consider the sequence $a_n = (-1)^n$. We could prove that it does not converge just using the definition, but we are going to see a way of proving it more easily. For that, we are going to study this sequence in more detail. Note that although the sequence itself does not converge, we can focus on the even terms (the 1's) in the sequence and see that they form a convergent sequence. The same goes for the odd terms. This observation introduces the following definition.

Definition 20.4. Given a sequence (a_n) and $n_1 < n_2 < \dots$ are natural numbers, the sequence $(a_{n_k})_{k \in \mathbb{N}} = \left(a_{n_1}, a_{n_2}, a_{n_3}, \dots\right)$ is called a **subsequence** of (a_n).

Example 20.5. Say

$$(a_n) = \left(1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\right).$$

Then $(1/4, 1/10, 1/16, 1/20, \dots)$ is a subsequence. However, $(1, 1, 1, 1, \dots)$ is not a subsequence because we are not allowed to repeat indices; also $(1/3, 1/2, 1, 1/4, \dots)$ is not a subsequence since we are not allowed to change the order of the indices.

Theorem 20.6. *If $(a_n) \to a$ then any subsequence of (a_n) converges to a.*

Proof. Assume $\left(a_{n_k}\right)$ is a subsequence of (a_n). We show that $(a_{n_k}) \to a$. Assume $\varepsilon > 0$. Take N such that $|a_n - a| < \varepsilon$ for all $n \geq N$. Assume that $k \geq N$. Then we know that $n_k \geq k$, and so $n_k \geq N$. Therefore $|a_{n_k} - a| < \varepsilon$. □

A consequence of this theorem is that if (a_n) has two subsequences coverging to two different limits then (a_n) does not converge. For example, $(0, 1, 0, 1, \dots)$ does not converge.

Definition 20.7. A sequence (a_n) is **monotone** if it is either decreasing or increasing. We say that it is decreasing if $a_{n+1} \leq a_n$ for all $n \in \mathbb{N}$, and we say that it is increasing if $a_{n+1} \geq a_n$ for all $n \in \mathbb{N}$.

Example 20.8. The sequence

$$\left(1, 1, \frac{1}{2}, \frac{1}{2}, \frac{1}{3}, \frac{1}{3}, \dots\right)$$

is decreasing, hence monotone. The sequence $(0, 1, 0, 1, \dots)$ is not monotone. The sequence $(1, 1, 1, 1, 1, \dots)$ is both increasing and decreasing.

Theorem 20.9 (Monotone convergence theorem)**.** *If (a_n) is monotone and bounded, then (a_n) converges.*

Proof. Assume (a_n) is increasing. Set $A = \{a_n | n \in \mathbb{N}\}$. We know that $a_1 \in A$ and so A is not empty. We also know that (a_n) is bounded, and so there is M such that $|a_n| \leq M$. So M is an upper bound for A. Then A has a least upper bound. Take $a = \sup(A)$. We want to prove $(a_n) \to a$. Assume $\varepsilon > 0$. Since a is the supremum of A, then $a - \varepsilon$ is not an upper bound for A and so there is $x \in A$ such that $a - \varepsilon < x$. Take N such that $x = a_N$. Then $a - \varepsilon < a_N \leq a$. Assume $n \geq N$. Then since the sequence is increasing we know that $a_N \leq a_n$. Then $a - \varepsilon < a_N \leq a_n \leq a$ since a is an upper bound. This shows that $|a_n - a| < \varepsilon$. □

Note that the last conclusion of the proof follows from the following general fact: we have that $|x - y| < \varepsilon$ if and only if $x - \varepsilon < y < x + \varepsilon$.

Going back to the sequence $(-1, 1, -1, \dots)$ we see that although it does not converge it still has some converging subsequences. Is it true that given any bounded sequence it is possible to find some susbequence which converges? The answer to this question is yes.

Theorem 20.10 (Bolzano-Weierstrass theorem)**.** *Any bounded sequence has a convergent subsequence.*

Definition 20.11. An **accumulation point** of a sequence (a_n) is a real number a to which some subsequence of (a_n) converges.

Using this definition we can see that the Bolzano-Weierstrass theorem tells us that any bounded sequence has an accumulation point.

Definition 20.12. A sequence (a_n) is **Cauchy** if for any $\varepsilon > 0$ there is N such that for all $n, m \in \mathbb{N}$ we have $|a_n - a_m| < \varepsilon$.

From assignment 17 you know that if a sequence converges then it is Cauchy. Is the converse true? It turns out that it is.

Theorem 20.13. *Any Cauchy sequence converges.*

Proof. Cauchy sequences are bounded (this is left as an exercise, and the proof is similar to the proof that convergent sequences are bounded). By Bolzano-Weierstrass, there is a subsequence $\left(a_{n_k}\right)$ that converges to a real number a. We will prove that $(a_n) \to a$. Assume $\varepsilon > 0$. Take N_1 so that for any k with $n_k \geq N_1$ we have $|a_{n_k} - a| < \varepsilon/2$, and take N_2 such that for any $n, m \geq N_2$ we have $|a_n - a_m| < \varepsilon/2$. Let $N = \max(N_1, N_2)$. Now assume $n \geq N$, and take k so that $n_k \geq N \geq N_1, N_2$. Let $m = n_k$. Then

$$|a_n - a| \leq |a_m - a| + |a_n - a_m| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Therefore $(a_n) \to a$. □

21. Monday, November 19

21.1. **The Bolzano-Weierstrass theorem.** We saw last time (without proof) that every bounded sequence has a convergent subsequence. For example, the sequence $(0,1,0,1,0,1,0,\dots)$ is bounded and not convergent; however, the subsequence $(1,1,1,1,1,\dots)$ converges. There are several ways to prove this. One way is take the interval where the sequence lies (which exists since the sequence is bounded) and split it in half; then, look at a side with infinitely many points, and repeat the process. By repeating this we obtain a convergent subsequence.

Another idea is as follows: find a subsequence that increases or decreases, and then show that it goes to a limit (this uses the monotone convergence theorem).

A third idea is to find a bound that is near infinitely many terms. The first idea is the proof used in the book, and the remaining two are exercises. Let's look at the second one. We'll start by proving a theorem.

Theorem 21.1. *Any sequence has a monotone subsequence.*

An idea to prove this is modeled after the third idea above; namely, consider an element and look at whether there are infinitely many terms above it. If the answer is yes, we add it to our subsequence, and if no we discard it; we then repeat the process. This process might not work because there might be no increasing subsequence, and in that case we would try the process for a decreasing subsequence. For this kind of process it's helpful to introduce a definition.

Definition 21.2. A **peak** of a sequence (a_n) is a term a_m such that $a_m \geq a_n$ for all $n \geq m$.

In term of peaks, we can prove Theorem 21.1 by considering a subsequence of peaks. Such a subsequence will be decreasing by definition. However, there might be no infinite number of peaks; in that case, there might be an infinite number of "valleys" (the opposite of peaks), but even in this case there might be only finitely many of those. In any case, if we assume that there are finitely many peaks $a_{m_1},\dots,a_{m_\ell}$ we can just consider a_n with $n > m_\ell$, knowing that it is not a peak. By definition this means that there exists $n' > n$ such that $a_{n'} > a_n$. Since $a_{n'}$ is not a peak either we can repeat the process, and so we end up with an increasing subsequence.

Having proved Theorem 21.1 we can readily prove the Bolzano-Weierstrass theorem:

Proof of Bolzano-Weierstrass. Assume (a_n) is bounded. Find a monotone subsequence (a_{n_k}). By the monotone convergence theorem (a_{n_k}) converges. □

Let's go back to the third proof idea, namely that of finding a bound close to infinitely many terms of (a_n). Consider the set

$$A = \{x \in \mathbb{R} \mid \text{there are infinitely many } a_n \text{ with } x < a_n\}.$$

In order to show that this set has a supremum we need to show it is nonempty and bounded. We know that A is nonempty since $-M-1 \in A$ (where $[-M,M]$ is the interval containing (a_n)). Moreover A is bounded above since M is an upper bound. Let $a = \sup(A)$. Consider the interval $(a-1,a+1)$. We claim that there is n_1 such that $a_{n_1} \in (a-1,a+1)$. In fact, a is the supremum and therefore $a-1$ is not an upper bound, and by definition of A there are infinitely many a_n such that $a_n > a-1$. Moreover, since a is a supremum we know that there are only finitely many a_n above $a+1$. So we can find a_{n_1} with $a_{n_1} \in (a-1, a+1)$. We repeat this step to find a_{n_2} such that $a_{n_2} \in (a-1/2, a+1/2)$, and in general find $a_{n_k} \in (a-1/k, a+1/k)$. Then the subsequence (a_{n_k}) converges to a.

22. Monday, November 26

Missed class :(The material of today's class can be found at `http://math.harvard.edu/~sebv/101-fall-2018/supreals.pdf` (note that the presentation is different than in Abbott's book).

23. Friday, November 30

Note that the last class on Monday, December 3 will be a review session. Bring questions!

23.1. **Representing real numbers: continuous fractions.** [2]

As we said previously, we can use decimal expansions to represent real numbers. For example, we can write

$$\begin{aligned}\sqrt{2} =& 1.4142135\ldots\\ e =& 2.71828182845\ldots\\ \pi =& 3.141592653\ldots\end{aligned}$$

and similarly for other numbers. However, we see that all these expansions look very irregular, but this concept is harder to express. In particular, how complicated are these numbers? Can we represent them in some other way? The answe is yes, and it will turn out that numbers such as $\sqrt{2}$ are less complicated than e or π.

Example 23.1. Consider, for example, the decimal expansion

$$x = \frac{19}{7} = 2.714285714285714285\ldots$$

We could write in a way that isolates the integer part:

$$\frac{19}{7} = 2 + \frac{5}{7}.$$

We could repeat this step with the reciprocal of the remainder, to obtain

$$\frac{1}{\frac{5}{7}} = \frac{7}{5} = 1 + \frac{2}{5};$$

if we keep going, we obtain

$$\frac{1}{\frac{2}{5}} = \frac{5}{2} = 2 + \frac{1}{2}$$

and here the remainder is the reciprocal of an integer, so that there are no more steps to take. If we combine all of these expansion, we can write

$$\frac{19}{7} = 2 + \frac{5}{7} = 2 + \frac{1}{\frac{7}{5}} = 2 + \frac{1}{1 + \frac{2}{5}} = 2 + \frac{1}{1 + \frac{1}{\frac{5}{2}}} = 2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{2}}}.$$

In general, any *rational number* $x \geq 1$ can be written as

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ddots_{a_{n-1} + \frac{1}{a_n}}}}.$$

[2] Good references for this topic include *The Real Numbers* by Stillwell and *Elementary Number Theory* by Stein (links can be found on the course website)

This is the **continued fraction** representation of x. For $x = 19/7$ we have $a_0 = 2, a_1 = 1, a_2 = 2, a_3 = 2$, and $n = 3$. The fact that there are only finitely many terms is due to the fact that the Euclidean algorithm terminates in a finite number of steps.

Example 23.2. Consider now the irrational number $\sqrt{2}$. We can proceed similarly as above, with the difference that in this case the integer part is going to be extracted by the floor function $\lfloor x \rfloor$, which by definition returns the largest integer n such that $n \leq x$. In this case, we see that

$$\begin{aligned}\sqrt{2} =& \lfloor \sqrt{2} \rfloor + \sqrt{2} - \lfloor \sqrt{2} \rfloor \\ =& 1 + \sqrt{2} - 1.\end{aligned}$$

We can repeat the same steps as in the previous example:

$$\begin{aligned}\frac{1}{\sqrt{2}-1} =& \frac{1}{\sqrt{2}-1} \cdot \frac{\sqrt{2}+1}{\sqrt{2}+1} \\ =& \frac{\sqrt{2}+1}{\sqrt{2}-1} \\ =& \sqrt{2}+1 \\ =& 2 + (\sqrt{2}+1-2) \\ =& 2 + (\sqrt{2}-1).\end{aligned}$$

In this case, the remainder is the same as the one in the previous step, so that the next step is going to be exactly the same. In conclusion,

$$\begin{aligned}\sqrt{2} =& 1 \frac{1}{\frac{1}{\sqrt{2}-1}} \\ =& 1 + \frac{1}{2 + \frac{1}{\sqrt{2}-1}} \\ =& 1 + \frac{1}{2 + \frac{1}{2+\frac{1}{2+\frac{1}{2+ \ddots}}}}.\end{aligned}$$

In particular, we see that $\sqrt{2}$ is not irrational.

Example 23.3. Let

$$\rho = \frac{1+\sqrt{5}}{2}$$

(also known as the golden ratio). Let's compute the continued fraction representation of ρ.

$$\begin{aligned}\rho =&\frac{1+\sqrt{5}}{2} = & \left\lfloor \frac{1+\sqrt{5}}{2} \right\rfloor + \rho - \lfloor \rho \rfloor \\ =&1+\rho-1 \\ =&1+\frac{\sqrt{5}-1}{2}.\end{aligned}$$

Moreover,

$$\begin{aligned}\frac{1}{\frac{\sqrt{5}-1}{1}} =&\frac{2(\sqrt{5}+1)}{5-1} \\ =&\frac{\sqrt{5}+1}{2} \\ =&\rho\end{aligned}$$

so that this brings us to the first step. Therefore

$$\rho =1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+ \ddots}}}.$$

Note that in the last two examples we have been very imprecise about what we mean by our continued fraction example. For example, we haven't defined what it means for the fraction to "go on," nor have we proved that such representation "approximates" the number it represents. The following definition is going to make these concept precise.

Definition 23.4. For $a_0, a_1, a_2, \dots \geq 1$ define

$$a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \dots}}$$

to be the limit (if it exists) of the sequence (c_n) where

$$c_n = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{n-1} + \frac{1}{a_n}}}}.$$

The term c_n is called the nth convergent.

Remark. Note that in general we write

$$\sum_{n=1}^{\infty} \frac{1}{n^2} \overset{\text{def}}{=} \lim_{m \to \infty} \sum_{n=1}^{m} \frac{1}{n^2}.$$

Example 23.5. For $\rho = \frac{1+\sqrt{5}}{2}$ we have

$$c_1 = 1, c_2 = \frac{2}{1}, c_3 = \frac{3}{2}, c_4 = \frac{5}{3},$$

and in general we can prove that c_n is going to be equal to F_{n+1}/F_n, where F_n is the nth Fibonacci number.

We can find other ways to express the term c_n. For instance, let $p_0 = a_0$ and $q_0 = 1$. Then

$$c_0 = \frac{p_0}{q_0}.$$

Moreover, we have

$$c_1 = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}.$$

Let $p_1 = a_0 a_1 + 1$ and $q_1 = 1$. In general for $n \geq 2$ let

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2}.$$

Then we can prove by induction that

$$c_n = \frac{p_n}{q_n}.$$

Moreover we can prove using induction that for any number n we have

$$c_n - c_{n-1} = \frac{(-1)^{n-1}}{q_n q_{n-1}}.$$

Note that from the formula we see that $q_0, q_1 \geq 1$, $q_2 = a_2 q_1 + q_0 \geq 1 \cdot 1 + 1 = 2$, and in general

$$q_n \geq n.$$

It follows that $q_n q_{n-1} \geq (n-1)^2$ and therefore

$$c_n - c_{n-1} \leq \frac{(-1)^{n-1}}{(n-1)^2} \to 0.$$

Also, note that

$$c_2 - c_1 = \frac{-1}{q_2 q_1} < 0$$

and so $c_2 < c_1$. Similarly we see that $c_3 > c_2$. For $n \geq 2$ we see that

$$\begin{aligned} c_n - c_{n-2} =& c_n - c_{n-1} + c_{n-1} - c_{n-2} \\ \geq& (-1)^n \frac{2}{q_{n-1} q_{n-2}}. \end{aligned}$$

This implies that $c_4 - c_2 > 0$ (and similarly for even n) and $c_3 - c_1 < 0$ (same for odd n). In particular, we have inequalities

$$a_0 = c_0 < c_2 < c_4 < \cdots < c_5 < c_3 < c_1,$$

which means that the odd convergents approximate our number by above while the even convergents approximate it from below. Let's focus now on these two sequences, namely (c_{2k}) and (c_{2k+1}), separately. Each of these sequences are bounded and monotone, and therefore converge. Let

$$\lim_{k \to \infty} (c_{2k}) = \alpha \qquad \lim_{k \to \infty} (c_{2k+1}) = \beta.$$

We know that

$$0 \leq |c_{2k+1} - c_{2k}| \leq \frac{1}{k^2} \to 0.$$

The squeeze theorem makes us conclude that $(c_{2k+1} - c_n) \to 0$. We can now apply the algebraic limit theorem to show that

$$0 = \lim_{k\to\infty}(c_{2k+1} - c_{2k}) = \left(\lim_{k\to\infty} c_{2k+1}\right) - \left(\lim_{k\to\infty} c_{2k}\right) = \alpha - \beta,$$

and therefore $(c_n) \to \alpha = \beta$.

For fun, we can compute

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{6+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{8+\ddots}}}}}}}}}}}.$$

The continued fraction of π lacks this regularity.

24. Monday, December 3

24.1. **Review.** Today's class is to review the material on the exam and especially to answer any question.

Q: Can we go over the triangle inequality?

24.2. **Triangle inequality.** A way to state the triangle inequality is that for real numbers x and y we have

$$|x+y| \leq |x| + |y|.$$

Another version is the following: for all real mumbers x, y, z we have

$$|x-z| \leq |x-y| + |y-z|.$$

Q: This inequality is often used in proofs involving ε, for example the algebraic limit theorem. Can we go over it?

24.3. **Algebraic limit theorem.** We can prove the agebraic limit theorem by using the squeeze theorem or by using the definition. Let's try the latter. We want to prove that if $(a_n) \to a$ and $(b_n) \to b$ then $(a_n + b_n) \to a + b$.

Proof. Assume $\varepsilon > 0$. We know that the end of the proof is going to conclude that

$$|a_n + b_n - (a+b)| < \varepsilon.$$

Seeing that there are sums and differences inside an absolute value we can try and use the triangle inequality. In particular, we can regroup

$$|a_n + b_n - (a+b)| = |(a_n - a) + (b_n - b)|$$

and use the triangle inequality to obtain

$$|(a_n - a) + (b_n - b)| \leq |a_n - a| + |b_n - b|.$$

Thus in order for the above sum to be less than ε we need to limit each summand appropriately. Since $(a_n) \to a$ and $(b_n \to b)$, for every $\varepsilon_1, \varepsilon_2 > 0$ we can choose $N_1 \in \mathbb{N}$ and $N_2 \in \mathbb{N}$ such that for all $n \geq N_1$ we have $|a_n - a| < \varepsilon_1$ and for all $n_2 \geq N_2$ we have $|b_n - b| < \varepsilon_2$. Set $\varepsilon_1 = \varepsilon/2$ and $\varepsilon_2 = \varepsilon/2$. Take $N = \max(N_1, N_2)$. Then if $n \geq N$ we have

$$\begin{aligned}|a_n + b_n - (a+b)| =& |(a_n - a) + (b_n - b)| \\ \leq& |a_n - a| + |b_n - b| \\ <& \varepsilon_1 + \varepsilon_2.\end{aligned}$$

□

24.4. **Accumulation points.** We saw that not all sequences converge; for example, the sequence $(0,1,0,1,0,1,0,1,0,1,\dots)$. However, this sequence has accumulation points, which by definition are limits of convergent subsequences. In this case the accumulation points are 1 and 0, and

$$\limsup(0,1,0,1,0,1,\dots) = 1 \qquad \liminf(0,1,0,1,0,1,\dots) = 0.$$

24.5. **Properties of** $\liminf$ **and** $\limsup$. For (a_n) a bounded sequence (recall this means that there exists $M > 0$ such that $|a_n| \leq M$, or equivalently $-M \leq a \leq M$) we have

1. $\liminf a_n \leq \limsup a_n$;
2. $\liminf a_n = \limsup a_n = a$ if and only if $\lim a_n = a$;
3. if there is a sequence (b_n) such that $a_n \leq b_n$ for all n, then $\liminf a_n \leq \liminf b_n$ and $\limsup a_n \leq \limsup b_n$.

The second point implies that we can check if a sequence converges by computing its $\liminf$ and $\limsup$.

24.6. **Squeeze theorem.** The squeeze theorem states that if $(a_n) \to \ell$, $(c_n) \to \ell$, and $a_n \leq b_n \leq c_n$, then $(b_n) \to \ell$. We can prove it using the definition, but we can also use one of the properties above.

Proof. Let's compute $\liminf b_n$. We know that $\ell = \liminf a_n$ and

$$\liminf b_n \leq \liminf c_n = \ell$$

so that $\liminf b_n = \ell$. We can show similarly that $\limsup b_n = \ell$, and therefore $(b_n) \to \ell$. □

Note that there are some useful ways to prove that two real numbers a and b are equal. For instance,

(a) $a = b$ if and only if $a \leq b$ and $b \leq a$;
(b) $a = b$ if and only if $|a - b| < \varepsilon$ for every $\varepsilon > 0$.

24.7. **Boundedness.** Note that in the above statement of the squeeze theorem we didn't rigorously prove that (b_n) is bounded, which is necessary to know that $\liminf b_n$ and $\limsup b_n$ exist. Indeed, we know that $|a_n| \leq M_1$ since it converges, and $|c_n| \leq M_2$ similarly. Take $M = \max(M_1, M_2)$. Then $-M \leq b_n \leq M$.

Note that sometimes it is easier to show that a bound exists and deduce that a limit exists rather than actually computing the limit and deducing that the sequence is bounded. For example, consider the sequence

$$\left(1, 1 + \frac{1}{4}, 1 + \frac{1}{4} + \frac{1}{9}, \ldots, \sum_{n=1}^{m} \frac{1}{n^2}, \ldots\right).$$

We can show that it is bounded by 2, but it's much harder to compute the limit (which is $\pi^2/6$).

24.8. **Strengthened squeeze theorem.** This stronger version states the following: assume $(a_n) \to \ell$ and $(c_n) \to \ell$, and more over assume that for every $\varepsilon > 0$ there exists $N \in \mathbb{N}$ such that for every $n \geq N$ we have

$$a_n - \varepsilon \leq b_n \leq c_n + \varepsilon.$$

Then $b_n \to \ell$.

Proof. We show that (b_n) is bounded. Take $\varepsilon = 1$, and take $N \in \mathbb{N}$ such that for all $n \geq N$ we have $a_n - 1 \leq b_n \leq c_n + 1$. Now take

$$M = \max(|b_1|, |b_2|, |b_N|, M_1 + 1, M_2 + 1),$$

where $M_1 = \max(a_n)$ and $M_2 = \max(c_n)$. Since

$$-M_1 - 1 \leq a_n - 1 \leq b_n \leq c_n + 1 \leq M_2 + 1$$

for all $n \geq N$ it follows that $\max(M_1 + 1, M_2 + 1)$ bounds b_n for $n \geq N$. Consider $M_0 = \max(|b_1|, |b_2|, \ldots, |b_N|)$ and $M_3 = \max(M_1+1, M_2+1)$. Then we see that for $M = \max(M_0, M_3)$ we have

$$|b_n| \leq M \quad \text{for all } n \in \mathbb{N}.$$

This show that (b_n) is bounded. Set $\ell_1 = \liminf b_n$ and $\ell_2 = \limsup b_n$. If we show that $\ell_1 = \ell_2$ then we are done. Assume $\varepsilon > 0$, and take N such that for all $n \geq N$ we have $a_n - \varepsilon \leq b_n \leq c_n + \varepsilon$. Then $\liminf(a_n - \varepsilon) \leq \liminf b_n \leq \liminf(c_n + \varepsilon)$ since accumulation points do not depend on the first few terms of the sequences (the ones before N). By the algebraic limit theorem this gives that

$$\ell - \varepsilon \leq \ell_1 \leq \ell + \varepsilon,$$

and therefore $|\ell_1 - \ell| \leq \varepsilon$ for all ε. It follows that $\ell_1 = \ell$, and similarly we can prove that $\ell_2 = \ell$. In conclusion $\ell = \ell_1 = \ell_2$, which proves the theorem. □

24.9. **Checking convergence.** There are many ways to check that a sequence converges or diverges. For instance:

- if you find the limit, it's converges;
- if it's unbounded, it diverges;
- if bounded and monotone, it converges;
- if it's Cauchy, it converges;
- if $\liminf = \limsup$.

Index