MATH 65, FALL 2021, NOTES

Contents

1.	Sets Sept 9	2
2.	Theorems and proofs. Quantifiers. September 14	6
3.	Propositional Logic, Sept 15	11
4.	Induction. September 20	15
5.	Sequences, recurrences and induction. September 22	19
6.	Functions, Sept 27	23
7.	Bijections, Sept 29.	26
8.	Cardinality, Oct 4.	28
9.	Counting problems, union of sets, October 6	34
10.	Counting problems: products and factorials, October 18.	37
11.	Combinations with repetition and the pigeonhole principle, Oct 20.	44
12.	Relations, equivalence relations, October 25	46
13.	Equivalence classes, October 27	50
14.	Partial Orders November 1	54
15.	Probability, November 3	58
16.	Conditional probability, random variables and expectation, Nov 8	61
17.	Introduction to graphs, November 15	66
18.	More graphs and subgraphs, November 17.	70
19.	Paths, November 22.	74
20.	Euler Graphs, November 29	77
21.	Trees, December 1	81
22.	Planar Graphs, December 6	85
23.	The four color problem and graph coloring, December 8.	91
24.	Limits of sequences, Cauchy sequences, Dec 8	94
25.	The real numbers, Dec 13	98

1. Sets Sept 9

We introduces the language of set theory which is the basic notation you will use reading and writing Mathematics

We need to start somewhere , so although this is not a proper definition, we call a collection of objects a **set**.

For example the set of all students in the class. We will normally denote sets with capital letters. We can describe sets in multiple ways listing their elements or by giving a property that their elements satisfy. When we list their elements, we write them between brackets. For example $A = \{a, b, c\}$ or we could say that A consists of the first three letters of the english alphabet.

There are some sets of numbers that are used over and over in Math and we reserve some particular letters to design them. For instance

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

will be the set of natural numbers. I like to assume that the natural numbers contain 0, although mathematicians are evenly divided on that issue. It is better when you use this symbol that you clarify what you mean.

Similarly, we use the symbols $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ for the sets of integers, rational numbers, real numbers and complex numbers respectively. So

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$$

$$\mathbb{Q} = \{\frac{a}{b} |\ a, b \in \mathbb{Z}, b \neq 0 \ \text{ and } \frac{a}{b} = \frac{c}{d} \text{ if } ad = bc\}$$

The set of real numbers $\mathbb{R}$ is the one you used in Calculus.

You may have seen complex number when trying to solve quadratic equations

$$\mathbb{C} = \{a + bi | a, b \in \mathbb{R}\}$$

it is endowed with a natural addition and multiplication. Addition is done component-wise, using the addition you know in the real numbers. Multiplication is defined using the associative, commutative and distributive properties and the rule that $i^2 = -1$.

When an object is part of the collection of objects forming a a set, we will say that it is an **element** of the set and we write the symbol $\in$ to indicate this.

Definition 1.1. When every element of a set A is also an element of another set B, we say that A is a **subset** of B and write $A \subseteq B$. This includes the possibility that the two sets are equal. If we do not want to allow for this option, we can write $A \subset B$ or more explicitly $A \subsetneq B$.

Example 1.2. (a) The number 2 is a natural number. We say that 2 is an element of the set of natural numbers and we can write $2 \in \mathbb{N}$.

(b) When we write $\{2\}$ we mean a set whose only element is the number 2. We will NOT write $\{2\} \in \mathbb{N}$. Instead we write $\{2\} \subseteq \mathbb{N}$.

(c) We have natural inclusions

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

In fact, all these sets are different, so we could also write

$$\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$$

(d) The empty set is the set that has no elements. It is denoted with the symbol $\emptyset$. So, $\emptyset = \{\ \}$.

Two sets are equal if they contain the same exact elements. This means that they are contained in each other. Conversely, if we have two sets A, B with $A \subseteq B, B \subseteq A$, then $A = B$.

Example 1.3. (a) Define

$$A = \{x \in \mathbb{R} \,|\, x^3 - 3x^2 + 2x = 0\}, B = \{0, 1, 2\}$$

Let us show that $A = B$.

First we show that $B \subseteq A$. As B is given as a finite collection of real numbers, we can just check that all elements in B satisfy the condition that is required for a real number to be in A. That is, we need to see that

$$0^3 - 3 \times 0^2 + 2 \times 0 = 0, 1^3 - 3 \times 1^2 + 2 \times 1 = 0, 2^3 - 3 \times 2^2 + 2 \times 2 = 0$$

These equalities are all satisfied, so $B \subseteq A$.

We now need to prove the converse inclusion. Essentially, this means solving the equation $x^3 - 3x^2 + 2x = 0$ and proving that the only possible solutions are $0, 1, 2$.

Factoring, we find

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

For a product to be 0, one of the factors needs to be zero. This leads us to $x = 0, x = 1, x = 2$.

(b) Define

$$C = \{x \in \mathbb{R} \,|\, x^3 - 3x^2 + 2x > 0\}, D = \{x \in \mathbb{R} \,|\, 0 < x < 1 \text{ or } 2 < x < \infty\}$$

Let us show that $C = D$.

We saw already that we can factor $x^3 - 3x^2 + 2x = x(x - 1)(x - 2)$. A product of three numbers is positive if all of them are positive or two of them are negative and one positive. Now, $x - 1 > 0$ is equivalent to $x > 1$, $x - 2 > 0$ is equivalent to $x > 2$ and of course $x > 0$ is equivalent to $x > 0$. So, all three factors are positive for $x > 2$ while two of the factors are negative and the third positive for $0 < x < 1$. Using interval notation as in Calculus, the two sets are $(2, \infty)$, $(0, 1)$ respectively. The set C is then composed of these two pieces. (we will introduce notation for this in a second) and this is precisely the way we defined D.

We introduce some basic operations on sets

Definition 1.4. Given two sets A, B the **union** of the sets is the set whose elements are in either A or B (or both)

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

The **intersection** of the sets is the set whose elements are in both A and B

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

Two sets are said to be **disjoint** if their intersection is the empty set.

The **difference** of two sets is the set of elements that are in the first and not the second

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

If the sets we are dealing with are contained in some universal set U, the **complement** of A is the set of elements in U not in A

$$\bar{A} = \{x \mid x \notin A\} = U - A.$$

Unions and intersections can be taken for several (more than two) sets, even for infinite collections.

Sets are often represented with Venn Diagrams where each set takes the shape of an oval and you shade the piece corresponding to the operation. Below is a similar representation using rectangles instead of ovals

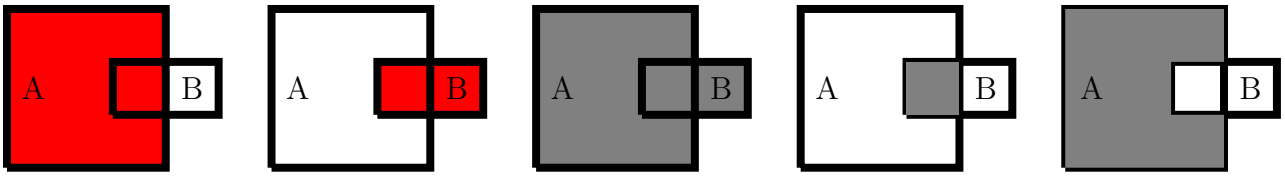


FIGURE 1. From left to right $A, B, A \cup B, A \cap B, A - B$

Example 1.5. (a) In example 1.5 b), $C = D = (0,1) \cup (2,\infty)$.

(b) The intersection $(0,1) \cap (2,\infty) = \emptyset$. So , the expression $C = (0,1) \cup (2,\infty)$ shows that C is the disjoint union of two open intervals in the real line.

(c) For every $n \in \mathbb{N} - \{0\}$ define the semiopen interval of the real line A_n by $A_n = -\frac{1}{n}, n]$. Then

$$\cap_{n\in\mathbb{N}-\{0\}} A_n = [0,1]$$

First $[0,1]$ is contained in each A_n and therefore in its intersection. Also any real number greater than 1 is not contained in A_1 and therefore not contained in the intersection of all A_n and any negative number is smaller than some $-\frac{1}{k}$ and therefore not in A_k and a fortiori, not in the intersection of all of the A_n. Similarly,

$$\cup_{n\in\mathbb{N}-\{0\}} A_n = (-1,\infty) :$$

No number smaller than or equal to -1 is in any A_k, therefore, it cannot be in its union. The numbers between -1 and 0 are in A_1 and therefore in the union. Any positive number is smaller than some natural number m and therefore it is in A_m.

Definition 1.6. Given two sets A, B the **cartesian product** of the sets is the set whose elements are pairs of elements the first one in A the second one in B:

$$A \times B = \{(x,y) \mid x \in A \text{ and } y \in B\}$$

Example 1.7. (a) You are already very familiar with at least one cartesian product. You know that the set of real numbers is represented geometrically as a real line. The cartesian product of two real lines is the set of pairs of real numbers. This is a representation of the points in the plane with each point determined by its two coordinates. That is $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ is a representation of the plane.

(b) If $A = \{x \in \mathbb{R} \,|\, x^3 - 3x^2 + 2x = 0\}, B = \{x \in \mathbb{R} \,|\, x^2 - 4 = 0\}$. We have seen that we can write $A = \{0,1,2\}$. Similarly, $B = \{2,-2\}$. Therefore,

$$A \times B = \{(0,2),(1,2),(2,2),(0,-2),(1,-2),(2,-2)\}$$

Definition 1.8. Given a set A the set of **parts of** A is the set consisting of all subsets of A.

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}$$

Example 1.9. (a) Take $A = \emptyset$. Then, $\mathcal{P}(\emptyset) = \{\emptyset\}$. This is a set whose only element is the empty set. In particular, $\mathcal{P}(\emptyset) \neq \emptyset$, as it contains one element.

(b) Take $A = \{1\}$. Then,

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

(c) Take $A = \{1, 2\}$. Then,

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

(d) We see from the previous examples that every time that we add a new element to a set, we double the number of elements in $\mathcal{P}(A)$. We should expect that if A has n elements, then $\mathcal{P}(A)$ has 2^n elements. We can see this as follows: when we construct a subset of A, for each of its elements, we need to decide whether it belongs or not to the subset. This gives two options for each element. These options can be combined in any arbitrary way, so there are in total 2^n possibilities.

2. Theorems and proofs. Quantifiers. September 14

In Mathematics, a Theorem is a statement that it is known to be true. A proof is a process by which you prove a Theorem. By this we mean that you start from some definitions and some results you know to be true or that you accepts as a basis (what are called "axioms") and from there with logical steps, you show that the result stated in the Theorem follows.

There is a hierarchy among Theorems, less important ones are usually called Propositions and Lemmas. The word Lemma is normally used for a result that will later be used to prove another result. But what is a Proposition, a Lemma or a Theorem varies depending on your point of view or your needs. This course is meant to make you acquainted with proof techniques that work in a number of settings. This does not mean that by the time you finish this course, you will be able to prove anything you want. Nobody knows how to prove everything. For example, in the year 2000, the Clay Institute gave a list of 7 Math problems `https://www.claymath.org/millennium-problems/millennium-prize-problems` with one million dollar award for the solution to each of them. So far, twenty years later, only one of them has been solved. People who claim to know how to write proofs apparently are not interested in any of the awards!.

Every problem requires specific ideas and methods. The more time you spend working out similar problems, the more likely you are to have seen something similar and come up with an idea that will help you in a proof.

Very often people thing a certain mathematical statement to be true when it turns out it is not. In this case what you need is not a proof but a counterexample to disprove the statement.

Fact 2.1. In this course, we will freely use the basic properties of addition and product of numbers in the sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ satisfy all the usual properties

(1) Associative, that is for all a, b, c in one of these sets $(a+b)+c = a+(b+c),\ a(bc) = (ab)c$.
(2) Commutative, that is for all a, b in one of these sets $a + b = b + a,\ ab = ba$.
(3) Existence of a 0 and a 1 with $a + 0 = a, a \times 1 = a$ for all a in these sets.
(4) Distributive property: for all a, b, c in any of these sets $a(b + c) = ab + ac$.
(5) Existence of inverses for addition in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, that is for all a on each of these sets, there is another element that we call $-a$ on the same set such that $a + (-a) = 0$.
(6) Existence of inverses for product in $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, that is for all $a \neq 0$ on each of these sets, there is another element that we call $\frac{1}{a}$ on the same set such that $a \times \frac{1}{a} = 1$.
(7) Order in $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ but not in $\mathbb{C}$: for any two different a, b, either $a < b$ or $b < a$ (and conversely, if $a < b$, then $a \neq b$). Moreover, if $a < b$ and $b < c$, then $a < c$.
(8) If $a < b$ and c is in the same set, then $a + c < b + c$. If $a < b$ and $c > 0$, then $ac < bc$.

Let us see some examples of proofs . We start with a couple of definitions

Definition 2.2. (a) An integer a is said to **divide** an integer b if there exists a third integer c such that $b = ac$. In this situation, we also say that b is divisible by a.
(b) An integer b is said to be **even** if 2 divides b. Equivalently, if there exists an integer c such that $b = 2c$.
(c) An integer b is said to be **odd** if there exists an integer c such that $b = 2c + 1$.

Let us start with the definitions above. We will also use some of the facts in 2.1, to show the following

Proposition 2.3. *(a) The sum of two even integers is even.*
(b) The sum of two odd integers is even.
(c) The sum of an even and an odd integer is odd.

Proof. (a) Assume that b_1, b_2 are even integers. From the definition, there exist integers c_1, c_2 such that $b_1 = 2c_1, b_2 = 2c_2$. Then,

$$\begin{aligned} b_1 + b_2 &= 2c_1 + 2c_2 && \text{for some } c_1, c_2 \in \mathbb{Z} \text{ by definition of even} \\ &= 2(c_1 + c_2) && \text{by the distributive property of addition with respect to multiplication} \\ &= 2c && \text{With } c = c_1 + c_2 \in \mathbb{Z} \text{ as the sum of integers is an integer} \end{aligned}$$

Now, the expression $b_1 + b_2 = 2c,\ c \in \mathbb{Z}$ shows, using the definition of even that $b_1 + b_2$ is even.

(b) The sum of two odd integers is even. Your should do the proof before reading on

Assume that b_1, b_2 are odd integers. From the definition, there exist integers c_1, c_2 such that $b_1 = 2c_1 + 1, b_2 = 2c_2 + 1$. Then,

$$\begin{aligned} b_1 + b_2 &= 2c_1 + 1 + 2c_2 + 1 && \text{for some } c_1, c_2 \in \mathbb{Z} \text{ by definition of odd} \\ &= 2c_1 + 2c_2 + 2 && \text{by the associative and commutative properties of addition} \\ &= 2(c_1 + c_2 + 1) && \text{by the distributive property of addition with respect to multiplication} \\ &= 2c && \text{With } c = c_1 + c_2 + 1 \in \mathbb{Z} \text{ as the sum of integers is an integer} \end{aligned}$$

Now, the expression $b_1 + b_2 = 2c,\ c \in \mathbb{Z}$ shows, using the definition of even that $b_1 + b_2$ is even.

(c) The sum of an even and an odd integer is odd:

Assume that b_1 is even and b_2 is odd. From the definition, there exist integers c_1, c_2 such that $b_1 = 2c_1, b_2 = 2c_2 + 1$. Then,

$$\begin{aligned} b_1 + b_2 &= 2c_+ 2c_2 + 1 && \text{for some } c_1, c_2 \in \mathbb{Z} \text{ by definition of odd} \\ &= 2(c_1 + c_2) + 1 && \text{by the distributive property of addition with respect to multiplication} \\ &= 2c + 1 && \text{With } c = c_1 + c_2 \in \mathbb{Z} \text{ as the sum of integers is an integer} \end{aligned}$$

□

Definition 2.4. (a) A natural number a is said to be **prime** if $a \neq 1$ and the only numbers that divide a are $1, a$.
(b) A natural number a is said to be **composite** if $a \neq 1$ and a is not prime.

Example 2.5. The number 6 is composite, the numbers 2 and 3 are prime.

Using the above definitions, we can show the following:

Proposition 2.6. *(a) If n is a natural number greater than or equal than 3, then $n^2 - 1$ is composite.*
(b) If n is a natural number greater than or equal than 2, then $n^3 + 1$ is composite.

Proof. (a) You are familiar with factoring the difference of two squares $n^2-1=(n-1)(n+1)$. This seems to suggest that n^2-1 is always composite, we can forget the conditions that n is greater than or equal than 3. But if you look carefully at the definition, you see that for a number to be composite, you do not only need a factorization, you also need both factors to be bigger than 1 (because if one of the factors is one, the other is the number itself). So, we need to add the condition $n-1>1$ or equivalently $n>2$. And because we are dealing with natural numbers, this is the same as saying $n\geq 3$. Then, if $n\geq 3$, $n+1\geq 4$, so the second factor will never be 1 and will fulfill the necessary condition on the definition of composite.

(b) Again we try to factor. We can actually write $n^3+1=(n+1)(n^2-n+1)$. We need $n+1>1$, which gives us again that n is at least 3. We also need $n^2-n+1>1$. Subtracting 1 from both sides, this is equivalent to $n^2-n>0$ or $n(n-1)>0$ which is true for any real number outside the interval $[0,1]$ and in particular, for every natural number greater than or equal to 3.

□

We now introduce notation for quantifiers. There are two symbols we will be using as follows

Definition 2.7. (a) The symbol $\forall$ means "for every element".
(b) The symbol $\exists$ denotes "exists ".
(c) The symbol $\exists!$ denotes "exists a unique element".

Example 2.8. (a) In Definition 2.2, one could write if $b\in\mathbb{Z}$ then b is said to be **even** if $\exists c\in\mathbb{Z}$ such that $b=2c$.

(b) The condition for the existence of additive inverse in the list of facts could be written as

$$\forall a\in\mathbb{Z},\exists(-a)\in\mathbb{Z} \text{ such that } a+(-a)=0$$

(c) We could have been more precise. The additive inverse is actually unique: if we have $a+(-a)=0,\ a+a'=0$, then

$$\begin{aligned}
a' &= 0+a' && \text{by the property of } 0\\
&=(a+(-a))+a' && \text{by the property of } -a\\
&=(-a)+(a+a') && \text{by the commutative and associative properties}\\
&= (-a)+0 && \text{by the assumption on } a+a'=0\\
&= -a && \text{by the property of } 0
\end{aligned}$$

So a' is just $-a$. We can therefore write the existence of additive inverse as

$$\forall a\in\mathbb{Z},\exists!(-a)\in\mathbb{Z} \text{ such that } a+(-a)=0$$

Sometimes we use several quantifiers in a sentence. The order in which we use them is important

Example 2.9. (a) Consider the two statements:

$$\forall a\in\mathbb{Z},\ \exists b\in\mathbb{Z} \text{ such that } a+b=0$$

$$\exists b\in\mathbb{Z} \text{ such that } \ \forall a\in\mathbb{Z},\ a+b=0$$

The first statement is true, it is the existence of inverse for addition. In Facts 2.1, condition 5, you take $b = -a$. You notice that this b depends on a. Now this is fine because once we fix our attention on a particular a, we choose the b that works.

The second statement though is false. We are claiming that we can find an inverse that is inverse of every element in $\mathbb{Z}$. While we can individually find additive inverses, no number will do the job for all integers at once.

(b) When the two quantifiers are of the same type, then the order does not matter. For example the two statements below are equivalent (and are true by the commutative property)

$$\forall a \in \mathbb{Z},\ \forall b \in \mathbb{Z},\ 3a + 5b = 5b + 3a$$
$$\forall b \in \mathbb{Z}\ \forall a \in \mathbb{Z},\ 3a + 5b = 5b + 3a$$

Similarly, the two statements below

$$\exists a \in \mathbb{Z} \text{ such that } \exists b \in \mathbb{Z} \text{ with } ab = 1$$
$$\exists b \in \mathbb{Z} \text{ such that } \exists a \in \mathbb{Z} \text{ with } ab = 1$$

are equivalent and true (taking $a = 1, b = 1$ or $a = -1, b = -1$.

Note that when you want to negate a sentence that contains a quantifier, you will need to change the quantifier

Example 2.10. (a) Think of the statement $\forall a \in \mathbb{Z},\ 2a > a$. This statement is false because there is at least one a that does not satisfy the condition. The statement that is correct is $\exists a \in \mathbb{Z},\ 2a \leq a$. We could take $a = -1$ to verify the statement.

(b) Think of the statement $\exists a \in \mathbb{N},\ 2a < a$. This statement is false because no natural number a satisfies the condition. The statement that is correct is $\forall a \in \mathbb{N},\ 2a \geq a$. This statement is equivalent to $a \geq 0$ and every natural number satisfies the condition.

(c) Think of the statement $\forall a \in \mathbb{Q}, \exists b \in \mathbb{Q}$ such that $ab = 1$. This statement is false because there is one $a \in \mathbb{Q}$ that does not satisfy the condition. The statement that is correct is $\exists a \in \mathbb{Q}$ such that $\forall b \in \mathbb{Q}, ab \neq 1$. We could take $a = 0$. Then for all b rational, $ab = 0 \neq 1$.

There are more properties of numbers that we use often. For example, on the first day we used that the product of two numbers is 0 precisely when one of the factors is 0. This follows in fact from

Proposition 2.11. *(a) For all $a \in \mathbb{R}$, if $a < 0$, then $-a > 0$.*
(b) For all $a \in \mathbb{R}$, $a \times 0 = 0$.
(c) For all $a \in \mathbb{R}$, if $-(a \times b) = a \times (-b) = (-a) \times b$..
(d) For all $a, b \in \mathbb{R}$, if $a \times b = 0$, then either $a = 0$ or $b = 0$.

Proof. (a) Assume $a < 0$. Using fact (7) from 2.1, we can add $-a$ to both sides and preserve the inequality: $a + (-a) < 0 + (-a)$. Using the properties of 0 and inverse (facts (3) and (5)), we obtain

$$0 = a + (-a) < 0 + (-a) = -a$$

(b) From Fact (3) in 2.1, we know that for all real numbers a, $a + 0 = a$. In particular, taking $a = 0$, we have that $0 + 0 = 0$.. Multiplying this identity with a, we have that $a \times (0+0) = a \times 0$. From the distributive property, we have that $a \times (0+0) = a \times 0 + a \times 0$. But we also know that $a \times (0+0) = a \times 0$. So, we deduce that $a \times 0 = a \times 0 + a \times 0$. We know

that every element has an additive inverse. This is true in particular for $a \times 0$. So, adding it to both sides of the equality, we have $a \times 0 + (-a \times 0) = [a \times 0 + a \times 0] + (-a \times 0)$. Now we will use the associative property, the property of 0 and the property of the additive inverse

$$\begin{aligned}
0 = & \quad a \times 0 + (-a \times 0) && \text{by the property of the additive inverse} \\
= & \ [a \times 0 + a \times 0] + (-a) \times 0 && \text{as we saw before} \\
= & a \times 0 + [a \times 0 + (-a) \times 0)] && \text{by the associative property} \\
= & \quad a \times 0 + 0 && \text{by the property of the additive inverse} \\
= & \quad a \times 0 && \text{by the property of 0}
\end{aligned}$$

(c) From the existence of inverse for addition, $a + (-a) = 0$. Multiplying both sides with b and using the distributive property $ab + (-a)b = 0b = 0$ Adding $-(ab)$ to both sides and using the commutative property

$$(-a)b = 0 + (-a)b = ab + -(ab) + (-a)b = 0 + (-(ab)) = -(ab)$$

(d) To prove (d), it suffices to see that if $a \neq 0, b \neq 0$, then $ab \neq 0$. When two numbers are different, according to fact (g), one of them is smaller than the other. As $b \neq 0$ by assumption, either $0 < b$ or $b < 0$. Let us assume first, that $0 < b$. Then, if $0 < a$, multiplying both sides by b and using fact (h) and what we already proved that $b \times 0 = 0$, we obtain $0 = b \times 0 < b \times a$. If $a < 0$, proceeding similarly $b \times a < 0$, so in both cases $b \times a \neq 0$. If $a > 0$, we could reason similarly. If both $a < 0, b < 0$, we have shown in (a) that $-a > 0, -b > 0$. therefore, from what we have already proved, $(-a)(-b) > 0$. But then, using (c) twice, $(-a)(-b) = -a(-b) = -(-(ab))$. From the definition of additive inverse, the inverse of the inverse is the original number $-(-(ab)) = ab$. Therefore $ab > 0$.

□

3. Propositional Logic, Sept 15

The goal of this section is to describe the logical underpinnings of Math writing. We start with a definition:

Definition 3.1. A proposition is a statement that is either true or false (and not both).

Example 3.2. (a) The statement "I will get an A in Math 65" is a proposition. For any of you at the moment, we do not know if it is true or false but it is one of the two (and, by the way, whether it is true or not depends on how much work you put into it). The statement "Give me an A in Math 61" is not proposition. It. is an order or suggestion that I will happily oblige by if you deserve it.

(b) The statement "3+5=7" is a proposition that we know is false. The statement "3+5-7" is not proposition, it is just an expression, neither true nor false.

(c) The statements " The square of each real number is strictly positive", " The square root of some real numbers is not a real number" are both propositions. The first one is false as the square of 0 is 0 which is not strictly positive. The second one is true as the square root of negative numbers is not a real number.

(d) The statement $x^2-4=0$ is not a proposition. The statement $\exists x \in \mathbb{R}$ such that $x^2-4=0$ is a proposition which is true as 2 is a real number and $2^2-4=0$. The statement $\forall x \in \mathbb{R}$ $x^2-4=0$ is a proposition which is false as 3 is a real number and $3^2-4=5\neq 0$.

We will now describe how to create new propositions from old ones. We can determine what a proposition means from its true or false values. If there are several independent propositions involved in a given combination, each of them can take a true or false value. The meaning of the combination can then be described from the value it takes in each case. This is often displayed on a table.

Definition 3.3. Given propositions p, q,

(a) The **negation** of p is written as $\neg p$ "no p". It is a proposition that is true when p is false and false when p is true.

(b) The **conjunction** of p, q is written as $p \wedge q$ "p and q". It is a proposition that is true when both p, q are true and false when at least one of p, q is false.

(c) The **disjunction** of p, q is written as $p \vee q$ "p or q". It is a proposition that is true when at least one of p, q are true and false when both p, q are false.

(d) The **conditional** of p, q is written as $p \Rightarrow q$ "p implies q". It is a proposition that is true when p is false and when both p, q are true. The conditional is false when p is true and q is false.

(e) The **biconditional** of p, q is written as $p \iff q$ "p if and only if q" or "p equivalent to q". It is a proposition that is true when both p, q are false and when both p, q are true. The biconditional is false when p, q have different truth values.

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \iff q$
T	T	F	T	T	T	T
T	F	F	F	T	F	F
F	T	T	F	T	T	F
F	F	T	F	F	T	T

Example 3.4. Let us consider the propositions p " I like hikes" q "tomato plants need at least 6 hours of sun a day", r " $3+5=8$ ", s " $3 \geq 8$ " .

(a) The proposition $\neg p$ would be " I do not like hikes" .
(b) The proposition $r \wedge s$ would be " $3 + 5 = 8$ and $3 \geq 8$" .
(c) The proposition $p \vee q$ would be "I like hikes or tomato plants need at least 6 hours of sun a day or both" .
(d) The proposition $r \Rightarrow s$ would be "If $3 + 5 = 8$ then $3 \geq 8$".
(e) The proposition $p \iff s$ would be "If I like hikes if and only if $3 \geq 8$" .

One can of course consider statements that involve three or more basic propositions such as for instance $(p \vee q) \wedge r$. A table to show the true values of such a statement will need to have 8 rows in order to combine all possible truth values for p, q, r.

Definition 3.5. Two statements are said to be **logically equivalent** if they take the same truth values for all possible truth values of the independent components.

A good way then to prove logical equivalence is by writing a truth table. Also, once you know some equivalences, you can use them to prove more in the same way you use a Lemma to prove a theorem. As and example, let us show that $(p \vee q) \wedge r$ is equivalent to $(p \wedge r) \vee (q \wedge r)$:

p	**q**	**r**	$\mathbf{p \vee q}$	$(\ \mathbf{p} \vee \mathbf{q})\wedge \mathbf{r}$	$\mathbf{p \wedge r}$	$\mathbf{q \wedge r}$	$(\ \mathbf{p} \wedge \mathbf{r}\ )\vee (\mathbf{q} \wedge \mathbf{r}\ )$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F
T	F	T	T	T	T	F	T
T	F	F	T	F	F	F	F
F	T	T	T	T	F	T	T
F	T	F	T	F	F	F	F
F	F	T	F	F	F	F	F
F	F	F	F	F	F	F	F

The most interesting logical equivalences for us will be the ones that allow us to prove things in different ways. In particular, we have the following:

Proposition 3.6. *(a) The conditional $p \Rightarrow q$ is equivalent to $\neg q \Rightarrow \neg p$ (contrapositive).*
(b) The conditional $p \Rightarrow q$ is equivalent to $\neg p \vee q$.
(c) The conditional $p \Rightarrow q$ is equivalent to $(p \wedge \neg q) \iff F$ (proof by contradiction). Here by F we mean a proposition that takes only the false value.
(d) The biconditional $p \iff q$ is equivalent to $(p \Rightarrow q) \wedge (q \Rightarrow p)$.

Proof. A proof can be obtained by just writing the truth table

p	q	F	$\neg p$	$\neg q$	$p \Rightarrow q$	$\neg q \Rightarrow \neg p$	$\neg p \vee q$	$p \wedge \neg q$	$(p \wedge \neg q) \iff F$
T	T	F	F	F	T	T	T	F	T
T	F	F	F	T	F	F	F	T	F
F	T	F	T	F	T	T	T	F	T
F	F	F	T	T	T	T	T	F	T

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$(p \Rightarrow q) \wedge (q \Rightarrow p)$	$p \iff q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

□

Let us see how we use these equivalences in some proofs. When two statements are logically equivalent, proving one proves also the other. For instance, in order to prove $p \Rightarrow q$ we can prove the logically equivalent statement $\neg q \Rightarrow \neg p$. This kind of proof is called a proof by **contrapositive**.

Example 3.7. (a) Let us show that in the set of real numbers, the function $f(x) = mx + b$ with $m \neq 0$ has no repeated images, that is no two real numbers map to the same real number. We can write this symbolically as follows

$$\forall x_1, x_2 \in \mathbb{R}, \text{ if } x_1 \neq x_2, \text{ then } f(x_1) \neq f(x_2)$$

If p is the proposition $x_1 \neq x_2$ and q is the proposition $f(x_1) \neq f(x_2)$, then the statement takes the form $p \Rightarrow q$. We will do a proof by contrapositive. We know that $p \Rightarrow q$ is logically equivalent to $\neg q \Rightarrow \neg p$. The proposition $\neg q \Rightarrow \neg p$ takes the form

$$\forall x_1, x_2 \in \mathbb{R}, \text{ if } f(x_1) = f(x_2), \text{ then } x_1 = x_2$$

Let us prove this statement: we assume we have two real numbers $x_1, x_2 \in \mathbb{R}$ such that $f(x_1) = f(x_2)$. From the definition of f, this means that

$$mx_1 + b = mx_2 + b$$

As we are in $\mathbb{R}$, each number has an additive inverse and we can subtract b from both sides and get

$$mx_1 = mx_2$$

As we were assuming $m \neq 0$, we can multiply this equality with the multiplicative inverse of m, namely $\frac{1}{m}$ and we obtain

$$x_1 = x_2$$

which is precisely what we were after.

(b) We want, to to show that if an integer is a square then two more than this integer is not a square. We can write this symbolically as follows

$$\forall n \in \mathbb{Z}, \text{ if } \exists a \in \mathbb{Z}, \text{ such that } x = a^2, \text{ then } \nexists b \in \mathbb{Z} \text{ such that } x + 2 = b^2$$

Fix an $n \in \mathbb{Z}$. Let p be the proposition $\exists a \in \mathbb{Z}$, such that $x = a^2$,. Let q be the proposition $\nexists b \in \mathbb{Z}$ such that $x + 2 = b^2$. We want to prove the statement $p \Rightarrow q$. We will do a proof by contradiction. We know that $p \Rightarrow q$ is logically equivalent to $(p \wedge \neg q) \iff F$. The statement $p \wedge \neg q$ takes the form

$$\exists a \in \mathbb{Z}, \text{ such that } x = a^2 \ \wedge \ \exists b \in \mathbb{Z} \text{ such that } x + 2 = b^2$$

Because $a^2 = (-a)^2, b^2 = (-b)^2$ we can assume both a, b to be positive. Because $b^2 = x + 2 > x = a^2$, $b > a$. Subtracting the two equations we are assuming, we obtain

$$2 = b^2 - a^2 = (b - a)(b + a)$$

As 2 is a prime number and both $b - a, b + a$ are positive integers with $b + a > b - a$, we have $b - a = 1, b + a = 2$. Adding these two, we get

$$2b = 3$$

which contradicts the fact that 3 is not even. We got a false statement which is what we were aiming for.

(c) The square root of 2 is not rational. Let p be the proposition $x = \sqrt{2}$. Let q be the proposition $x \notin \mathbb{Q}$. We want to prove the statement $p \Rightarrow q$. We will do a proof by contradiction. We know that $p \Rightarrow q$ is logically equivalent to $(p \wedge \neg q) \iff F$. The statement $p \wedge \neg q$ takes the form

$$x = \sqrt{2} \ \wedge \ x \in \mathbb{Q}$$

Equivalently,

$$\sqrt{2} \in \mathbb{Q}$$

Rational numbers are of the form $\frac{a}{b}$. So, with our assumptions, $\sqrt{2} = \frac{a}{b}$ and we can assume a, b do not have prime factors in common. Then squaring

$$2 = \frac{a^2}{b^2}$$

So, $2b^2 = a^2$. Then 2 is a prime number and it divides a^2. The prime factors of a^2 are the same as the prime factors of a, just with twice the exponent. Hence, 2 must divide a. Then, $a = 2c$, so $2b^2 = a^2 = 4c^2$. Dividing both sides by 2, $b^2 = 2c^2$. Then 2 divides b which is not compatible with 2 divides a and a, b do not have prime factors in common. We got a false statement as we were aiming for.

If you are a computer science major, you may be interested on how logical equivalences are used in computer science. I am not an expert on the topic and your CS faculty will be better at giving you references but here is something to look at if you wish

`https://en.wikipedia.org/wiki/NAND_gate`
`https://en.wikipedia.org/wiki/Functional_completeness`

4. Induction. September 20

Induction is a method that allows you to prove some types of statements that are given for each of the natural numbers. For example, we showed earlier in the class that if a set A_n has n elements, then $\mathcal{P}(A_n)$ has 2^n elements.

The basis for the proof is the following claim that we will be using

Remark 1. *Every non-empty subset of the set of natural numbers has a minimum element.*

This remark is only true for the natural numbers. It fails for instance in the set of integers: the set of even numbers does not have a minimal element as $-2, -4, -6, \ldots$ are all even. It is even worse for rational and real numbers. In the set of rational and real numbers, even if a set is bounded below, it does not need to have a minimal element. For example, the open interval of the real line $(0, 1)$ does not have a minimal element because 0 is not in the set but we can get as close to 0 as we want.

Proposition 4.1 (Induction Principle)**.** *Given a statement $X(n), n \in \mathbb{N}, n \geq k$. we can prove it is correct with the following two steps*

- **Step 1:** *Check directly that $X(k)$ is correct.*
- **Step 2:** *Check that $X(n-1) \Rightarrow X(n)$ for $n - 1 \geq k$ or equivalently for $n \geq k + 1$..*

Then, we have shown that $X(n)$ is true for all natural numbers $n \geq k$

Proof. The idea is that if the statement failed for some value (greater than or equal to k), we could go back and find the smallest value for which it fails. We checked that the statement works for k, so the value for which it fails needs to be bigger. But then if we chose the smallest of the values for which it fails, the result is true for the previous one. Hence, from the second condition, it is also true for the next, contradicting that we were assuming it was false.

Let us write the details of this argument formally: We are able to check the two statements

- **Step 1:** Statement p " $X(k)$ is correct."
- **Step 2:** Statement q, "$\forall n \geq k + 1,\ X(n-1) \Rightarrow X(n)$".

We want to show that $p \wedge q$ imply statement r, "$\forall n \geq k, X(n)$ is true".

We use a proof by contradiction. This means that we assume $\neg r \wedge (p \wedge q)$ and we get that something goes completely wrong.

The negation of r, "$\forall n \geq k, X(n)$ is true" is "$\exists m \geq k, X(m)$ is false". This can be stated as the non-emptiness of the following set

$$A = \{n \in \mathbb{N} | n \geq k \text{ and } X(n) \text{ is false } \} \neq \emptyset$$

We assume that $A \neq \emptyset$, $X(k)$ is correct and $\forall n \geq k + 1,\ X(n-1) \Rightarrow X(n)$ and get that something goes wrong.

From Remark 1,the set A ha a minimum element, let us call it m. From the definition of A, and the assumption that $X(k)$is correct, $k \notin A$, so, as m **is** in A, we need to have $m \geq k + 1$. From our choice of m as the minimum in A, $m - 1 \notin A$. Then, the definition of A means that $X(m-1)$ is true. From the second assumption, it follows that $X(m)$ is also true contradicting our choice $m \in A$. Therefore A is empty and the result is proved. □

Example 4.2. (a) Show that if A_n has n elements then the set of subsets of A_n denoted by $\mathcal{P}(A_n)$ has 2^n elements.

- **Step 1:** Check the result for $n = 0$. For $n = 0, A_0 = \emptyset$. Its only subset is the empty set itself. Hence
$$\mathcal{P}(A_0) = \mathcal{P}(\emptyset) = \{\emptyset\}$$
So, the set of subsets of A_0 has one element only. As $2^0 = 1$, this is what we need. The result is checked for $n = 0$.
- **Step 2:** Assume the result correct for $n - 1$, that is a set with $n - 1$ elements has 2^{n-1} subsets. Let us prove that a set with n elements has 2^n subsets.
A subset of A_n either contains the element n or it doesn't. If it does not contain the element n, then it is a subset of A_{n-1}. By our induction assumption, there are 2^{n-1} such subsets.
If it **does** contain the element n, then it is made of a subset of A_{n-1} to which we add the element n. By our induction assumption, there are 2^{n-1} such subsets.
Adding the number of subsets that do not contain the element n with the number of subsets that do, we have that the total number of subsets of A_n is
$$2^{n-1} + 2^{n-1} = 2 \times 2^{n-1} = 2^n$$
This agrees with our expectations.

As both step 1 and step 2 work, we can now claim that $\mathcal{P}(A_n)$ has 2^n elements.

(b) Show that $S = 0 + 1 + 2 + 3 + \cdots + (n-1) + n = \frac{n(n+1)}{2}$.

This can be shown without using induction as follows: we write this sum S twice, once in ascending order and once in descending order

$$\begin{array}{ccccccccccc} 0 & + & 1 & + & \ldots & + & (n-1) & + & n \\ n & + & n-1 & + & \ldots & + & 2 & + & 1 \end{array}$$

If we add each term in the second row to the one above it, we get always n. There are $n + 1$ terms in S. So twice S is $n(n + 1)$. Then $S = \frac{n(n+1)}{2}$.

We now do a proof by induction:

- **Step 1:** Check the result for $n = 0$: $0 = \frac{0(0+1)}{2}$.
- **Step 2:** Assume the result correct for $n - 1$, that is the sum with a fewer term takes the same form (replacing n with $n - 1$):

$$S_{n-1} = 0 + 1 + 2 + 3 + \cdots + (n-2) + (n-1) = \frac{(n-1)((n-1)+1)}{2} = \frac{(n-1)n}{2}.$$

Now,

$$S = S_{n-1} + n = \frac{(n-1)n}{2} + n = \frac{(n-1)n}{2} + \frac{2n}{2} = \frac{(n-1+2)n}{2} = \frac{(n+1)n}{2}$$

proving the result.

(c) Let $n \in \mathbb{N}$. Then, $4^n - 1$ is divisible by 3.

We now do a proof by induction:

- **Step 1:** Check the result for $n = 0$: $4^0 - 1 = 1 - 1 = 0 = 3 \times 0$ is divisible by 3.
- **Step 2:** Assume the result correct for $n - 1$, that is, there exists an integer k such that $4^{n-1} - 1 = 3k$.

We need to check that $4^n - 1$ is also divisible by 3. We can write

$$4^n - 1 = 4 \times 4^{n-1} - 1 = 4 \times (4^{n-1} - 1) + 4 - 1 = 4 \times 3c + 3 = 3(4c + 1)$$

As c is an integer, $4c+1$ is also an integer. This proves that $4^n - 1$ is also divisible by 3. By the principle of induction, the result is true for all n.

Proposition 4.3 (Strong Induction Principle)**.** *Given a statement $X(n), n \in \mathbb{N}$. we can prove it is correct with the following two steps*

- **Step 1:** *Check directly that $X(0)$ is correct.*
- **Step 2:** *Check that $X(k)$ correct for all $k < n \Rightarrow X(n)$.*

Then, we have shown that $X(n)$ is true for all natural numbers.

Proof. Again we prove it by contradiction. Assume that $\exists m \in \mathbb{N}$ such that $X(m)$ false. Then, the set

$$A = \{n \in \mathbb{N} | X(n) \text{ is false } \} \neq \emptyset$$

From Remark 1,the set A ha a minimum element, let us call it m. From the definition of A, and the first assumption, $0 \notin A$, so $m \geq 1$. From our choice of m as the minimum in A, $0, 1, \ldots, m-1 \notin A$ and therefore $X(k)$ is true for all $k < m$. Then, from the second assumption, $X(m)$ is also true contradicting our choice $m \in A$. Therefore A is empty and the result is proved. □

The difference between induction and strong induction is that in the second step, we are using more than the statement for the previous natural number, we are using it for all the previous natural numbers. In doing the proof, we need to be careful that we are not inadvertenly using the correctness of the statement for negative numbers, something we have not checked or assumed and therefore cannot use. This will often require that we check more than one case directly as in step 1 or with some separate argument

Proposition 4.4. *Given $n, b \in \mathbb{N}, b > 0$, there exist natural numbers q, r with $0 \leq r < b$ such that $n = bq + r$.*

Proof. Fix b a strictly positive natural number. We prove the result by strong induction

- **Step 1:** Check directly that q, r exist when $n = 0$. In fact, we can write $0 = 0 \times b + 0$, so $q = 0, r = 0$ satisfy the condition.
- **Step 2:** Show that if the statement is correct for all natural numbers less than n, it is also true for n.

Step 2 is easy to carry out if $n \geq b$:

If $n \geq b$, then $n - b \geq 0$. So, $n - b \in \mathbb{N}$. From our assumptions that the result id correct for all natural numbers less than n, there exist natural numbers q', r' with $0 \leq r < b$ such that $n - b = q'b + r'$. Then, $n = q'b + r' + b = (q' + 1)b + r'$. Taking $q = q' + 1 \in \mathbb{N}, r' = r$, we obtain the result for n as well. And if course, $r' = r$ still satisfies the condition that $0 \leq r < b$.

This proof does not work though if $n < b$ as then $n - b$ is negative and we do not know that the result applies to negative numbers. It is easy enough though to check the result directly in this situation: if n is a natural number with $n < b$, then $0 \leq n < b$. Taking $q = 0, r = b$, the identity $n = 0 \times b + n$ is identically correct and is an expression of the type we were looking for. □

Corollary 4.5. *Given $z, b \in \mathbb{Z}, b > 0$, there exist integers q, r with $0 \leq r < b$ such that $z = bq + r$.*

Proof. From Proposition 4.4, we already know the result if $z \geq 0$. Assume then $z < 0$. Then $-z > 0$. Hence, from Proposition 4.4, there exist natural numbers q', r' with $0 \leq r' < b$ such that $-z = bq' + r'$. Therefore, $z = b(-q') + (-r')$. Here $-q' \in \mathbb{Z}$. If $0 \leq r' < b$, multiplying with -1 that is a negative number we reverse the inequalities.Therefore $-b < -r' \leq 0$. If $r' = 0$, this is what we need. If r' is not 0, $-b < -r' < 0$. we can add b to these inequalities to give us $0 < b - r' < b$. From $z = b(-q') + (-r')$, we also have $z = b(-q' - 1) + (b - r')$. Then $q = -q' - 1, r = b - r'$ work in the statement of the corollary. □

Recall that we defined an integer a to be even if there exists another integer b such that $a = 2b$. We defined an integer a to be odd if there exists another integer b such that $a = 2b + 1$. This is the definition we will always use. Some people though define an integer as odd if it is not even. Let us check that the two definitions agree.

Corollary 4.6. *Every integer is either even or odd and not both. Equivalently, an integer is odd if and only if it is not even.*

Proof. The fact that every integer is even or odd follows from 4.5, taking b=2. For natural numbers, we can also show it directly from the strong induction principle in Proposition 4.3:

- **Step 1:** Check directly for $n = 0 = 2 \times 0$.
- **Step 2:** Show that if the statement is correct for all natural numbers less than n, it is also true for n. So, we assume that $n \geq 1$ and $n - 1$ is either even or odd. This means that there exists some integer c such that either $n - 1 = 2c$ or $n - 1 = 2c + 1$. Then $n = 2c + 1$ or $n = 2c + 2 = 2(c + 1)$. In the first case, n is odd. In the second case, as $c + 1$ is also an integer, n is even.

For negative integers, it follows from the case for positive ones: if $n < 0$, then $-n > 0$. Therefore, there exists and integer c such that $-n = 2c$ or $-n = 2c + 1$. It follows that $n = 2(-c)$ or $n = -2c - 1 = 2(-c - 1) + 1$, showing that the number is even or odd.

It remains to check that no number is both even and odd: Assume that n is both even and odd. Then for some integers c, d, $n = 2c = 2d + 1$. It follows that $1 = 2(c - d)$. As c, d are integers, $c - d$ is an integer. As 1 is positive, $c - d$ is positive. Hence, $c - d \geq 1$. But then $1 = 2(c - d) \geq 2$ which is impossible. □

5. Sequences, recurrences and induction. September 22

Definition 5.1. A sequence $a_n, n \in \mathbb{N}$ is. a collection of (say real) numbers, one for every natural number.

Example 5.2. (a) The sequence $0, 1, 2, \ldots$ corresponds to $a_n = n$.
(b) The sequence $1, -1, 1, -1, \ldots$ corresponds to $a_n = (-1)^n$.
(c) The sequence $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, , \ldots$ corresponds to $a_n = \frac{1}{n+1}, n \in \mathbb{N}$ or $b_n = \frac{1}{n}, n \in \mathbb{N} - \{0\}$.

One can sometimes define a sequence recursively.

Example 5.3. (a) For instance, in example 5.3 (a), the sequence is determined by saying that $a_0 = 0, a_n = a_{n-1} + 1$. It is clear that the sequence we wrote satisfies the two conditions $a_0 = 0, a_n = a_{n-1} + 1$.

We can use induction on n and check that if a sequence b_n satisfies the two conditions $b_0 = 0, b_n = b_{n-1} + 1$, then $b_n = n$:

- Step 1 We need to check that $b_0 = 0$ but this is one of the conditions, so it will be satisfied.
- Step 2, We need to check that if $b_{n-1} = n - 1$, then $b_n = n$. This follows from the second condition $b_n = b_{n-1} + 1$.

Then, induction tells us that $b_n = n$ for all n.

(b) Let $a_n, n \in \mathbb{N}$ be a sequence satisfying $a_0 = 3, a_n = 2a_{n-1}$. then, we claim that $a_n = 3 \times 2^n$.

We can use induction on n and check that if a sequence b_n satisfies the two conditions $b_0 = 3, b_n = 2b_{n-1}$, then $b_n = 3 \times 2^n$:

- Step 1 We need to check that $b_0 = 3 \times 2^0 = 3 \times 1 = 3$ but this is one of the conditions, so it will be satisfied.
- Step 2, We need to check that if $b_{n-1} = 3 \times 2^{n-1}$, then $b_n = 3 \times 2^n$. This follows from the second condition $b_n = 2b_{n-1} = 2 \times 3 \times 2^{n-1} = 3 \times 2^n$.

Then, induction tells us that $b_n = 3 \times 2^n$ for all n.

Example 5.4. (a) Show that the sequence $a_n = 2^n$ satisfies $a_n = 6a_{n-2} - a_{n-1}$.
(b) Show that the sequence $b_n = (-3)^n$ satisfies the recurrence $b_n = 6b_{n-2} - b_{n-1}$.
(c) There is only one sequence that satisfies all of the conditions below

$$c_0 = 1,\ c_1 = 7,\ \ c_n = 6c_{n-2} - c_{n-1},\ n \geq 2$$

(d) The only sequence that satisfies all of the conditions below

$$c_0 = 1,\ c_1 = 7,\ \ c_n = 6c_{n-2} - c_{n-1},\ n \geq 2$$

is $c_n = 2^{n+1} - (-3)^n$.

Let us check one condition at a time

(a) We need to check that the sequence $a_n = 2^n$ satisfies $a_n = 6a_{n-2} - a_{n-1}$. We just plug in the equation. We have

$$6a_{n-2} - a_{n-1} = 6 \times 2^{n-2} - 2^{n-1} = 2^{n-2}(6 - 2) = 4 \times 2^{n-2} = 2^n = a_n.$$

(b) To check that the sequence $b_n = (-3)^n$ satisfies the recurrence $b_n = 6b_{n-2} - b_{n-1}$, we just plug in

$$6b_{n-2} - b_{n-1} = 6 \times (-3)^{n-2} - (-3)^{n-1} = (-3)^{n-2}(6 - (-3)) = 9 \times (-3)^{n-2} = (-3)^n = b_n.$$

(c) Assume that there are two sequences c_n, d_n that satisfy

$$c_0 = 1,\ c_1 = 7,\ c_n = 6c_{n-2} - c_{n-1},\ n \geq 2,\quad d_0 = 1,\ d_1 = 7,\ d_n = 6d_{n-2} - d_{n-1},$$

We want to check that $c_n = d_n$. It makes sense that if we are given the first two terms and each term of the sequence is determined by the prior 2, there should be at most one possible sequence satisfying these conditions. We will use strong induction to prove it.

- Step 1 We need to check that $c_0 = d_0$. This is part of the assumption. In fact,we have a little more.We also know that $c_1 = d_1$ which is going to come in handy.
- Step 2, We need to check that if $d_k = c_k$ for all $k < n$, then also $c_n = d_n$. As we already know that $c_0 = d_0$ and $c_1 = d_1$, we can assume that $n \geq 2$. Then, using that $c_{n-2} = d_{n-2}, c_{n-1} = d_{n-1}$

$$c_n = 6c_{n-2} - c_{n-1} = 6d_{n-2} - d_{n-1} = d_n$$

Then, by strong induction, the result works for all n.

(d) We check that the given sequence c_n satisfies all three conditions We need to check that $c_0 = 3, c_1 = 7$. From the explicit description of c_n,

$$c_0 = 2^1 - (-3)^0 = 2 - 1 = 1,\ c_1 = 2^2 - (-3)^1 = 7$$

which is what we need. Then, we need to check that $c_n = 6c_{n-2} - c_{n-1}$. We can write $c_n = 2a_n - b_n$. We know that both sequences $(a_n), (b_n)$ satisfy the condition. Then,

$$6c_{n-2} - c_{n-1} = 6(2a_{n-2} - b_{n-2}) - (2a_{n-1} - b_{n-1}) = 2(6a_{n-2} - a_{n-1}) - (6b_{n-2} - b_{n-1}) = 2a_n - b_n = c_n$$

This checks that c_n satisfies the conditions.

Example 5.5. Consider the recurrence equation $a_n = a_{n-1} + 4a_{n-2} - 4a_{n-3}$ We would like to answer the following questions

(a) Assume that b is a real number different from zero. Can the sequence $a_n = b^n$ be a solution to the recurrence? (and if so for which values of b).
(b) Are there any solutions to the recurrence that satisfy $a_0 = 3, a_1 = 1, a_2 = 9$?
(c) Are there any solutions to the recurrence that satisfy $a_0 = 3, a_1 = 1, a_2 = 9, a_3 = 2$?

Let us try to answer these questions:

(a) We assume that the sequence $a_n = b^n$ satisfies $a_n = a_{n-1} + 4a_{n-2} - 4a_{n-3}$. Plugging in $a_n = b^n, a_{n-1} = b^{n-1}, a_{n-2} = b^{n-2}, a_{n-3} = b^{n-3}$, we obtain

$$b^n = b^{n-1} + 4b^{n-2} - 4b^{n-3} \iff b^n - b^{n-1} - 4b^{n-2} + 4b^{n-3} = 0 \iff b^{n-3}(b^3 - b^2 - 4b + 4) = 0$$

As we are assuming $b \neq 0$, this means $b^3 - b^2 - 4b + 4 = 0$. We can factor

$$b^3 - b^2 - 4b + 4 = (b-1)(b-2)(b+2).$$

Therefore, $b = 1, b = -2, b = 2$ are solutions of the stated form.

(b) We know that the sequences $a_n = 1, a_n = 2^n, a_n = (-2)^n$ are solutions of the recurrence. Then also any sequence of the form $a_n = x \times 1 + y \times 2^n + z \times (-2)^n$ for real numbers x, y, z is a solution. We can compute x, y, z so that $a_0 = 3, a_1 = 1, a_2 = 9$. We obtain $x = 1, y = 1, z = 1$.

(c) From the expression for a_n in terms of $a_{n-1}, a_{n-2}, a_{n-3}$ the first three terms of the sequence a_0, a_1, a_2 completely determine the sequence. So, as we saw before, if a solution were to exist with the given condition if would be given by $a_n = 1 + 2^n + (-2)^n$ which has the

right values of a_0, a_1, a_2. But then $a_3 = 1 + 2^3 + (-2)^3 = 1 \neq 2$. Therefore, there is no sequence satisfying $a_n = a_{n-1} + 4a_{n-2} - 4a_{n-3}, a_0 = 3, a_1 = 1, a_2 = 9, a_3 = 2$.

Example 5.6. We will call a shape made of 3-identical unit squares forming the shape of an L a basic L shape. An n-sized L shape will consist of $3n^2$ unit squares arranged as an L. The figure below shows a basic L shape and a 3-sized L-shape. Our goal is to show the followinng

(a) A $2 \times n$ rectangle can be completely covered by non-overlapping basic L shapes if and only if n is divisible by 3.
(b) Every n-sized L-shape can be completely covered by non-overlapping basic L shapes.

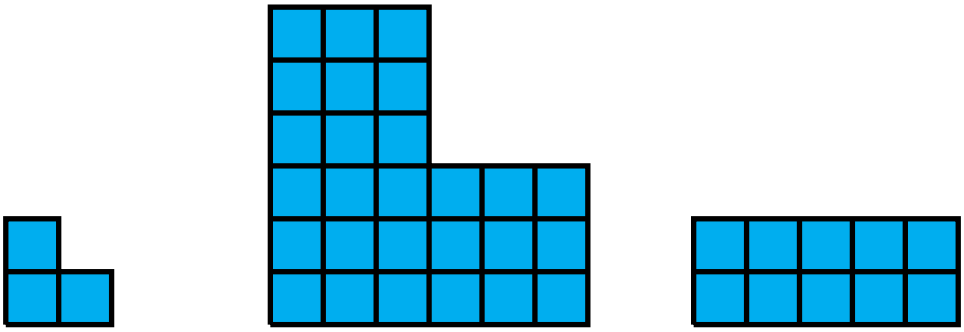


FIGURE 2. A basic L-shape and a 3-dimensional L-shape and a 2×5 rectangle.

Proof. (a) A $2 \times n$ rectangle is made of $3n$ squares. A basic L-shape is made up of 3 squares. If the rectangle can be completely covered by non-overlapping basic L shapes, $2n$ needs to be divisible by 3. As $2, 3$ are relatively prime, this requires that n is divisible by 3.

To prove the converse, if $n = 3k$ is divisible by 3, a $2 \times n$ rectangle is made of k 2×3 rectangles. Each 2×3 rectangle can be covered by 2 basic Lshapes. Then the whole rectangle can also be covered with non-overlapping basic L shapes.

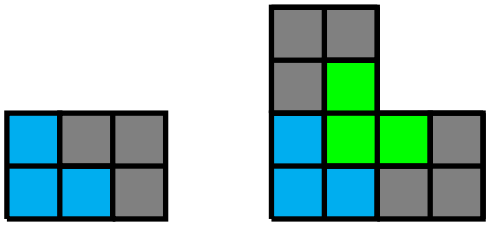


FIGURE 3. A 2×3 rectangle and a 2-sized L-shape covered by L-shapes

(b) In order to prove that every n-sized L-shape can be completely covered by non-overlapping basic L shapes, we use strong induction.
- Step 1 The case $n = 1$ is clear, as a 1-sized L-shape is a basic L shape.The case $n = 2$ is illustrated in the picture above.
- Step 2, We need to check that if the result is true for every $k < n$, then it is also true for n. We can assume $n > 2$, as the first two cases have already been checked. Remove from the n-sized L-shape a 2-sized L-shape with corner on the lower left corner and an $n - 2$-sized L-shape right above it (see Figure 4).

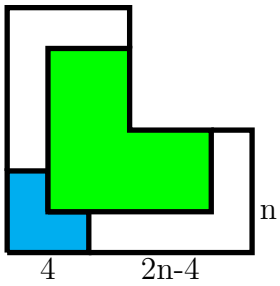


FIGURE 4. Remove from the L-shape a 2-L shape in the lower corner and an $n-2$ L-shape right above it.

The rest of the region consists of two pieces with similar shapes one at the top and the other at the right (white pieces in the picture). They can then be divided in $2 \times m$ rectangle with m divisible by 3 with suitable choices that depend on n. We describe the ones for the right white piece (see Figure 5):
If n is divisible by 3, so is $2n-6$. Form a vertical rectangle of height n and width 2 and a horizontal one of height 2 and width $2n-6$.
If $n-2$ is divisible by 3, so is $2n-4$. Form a vertical rectangle of height $n-2$ and width 2 and a horizontal one of height 2 and width $2n-4$.
If $n-1$ is divisible by 3, so are $n-4, 2n-8$. Form a vertical rectangle of height $n-4$ and width 2, a 2-dimensional L shape in the bottom left corner and a horizontal rectangle of height 2 and width $2n-8$.

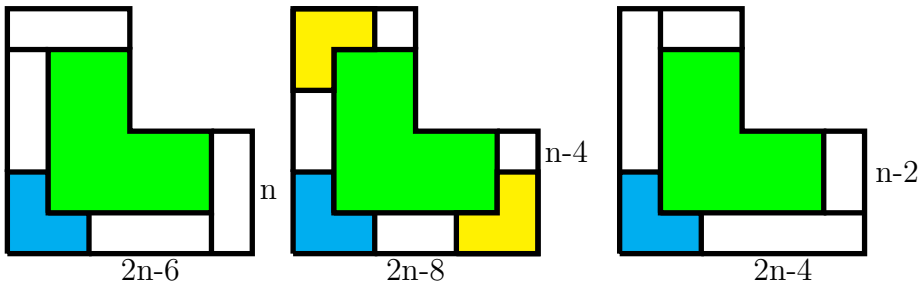


FIGURE 5. Subdivision of the left over rectangles corresponding to $n, n-1, n-2$ divisible by 3 respectively

□

.

6. Functions, Sept 27

Functions are the way in which sets relate to each other. We start with the definition:

Definition 6.1. A **function** consists of three pieces of data two sets A, B and a rule f that assigns to every element in A one and only one element in B. The set A is called the **domain**, the set B is called the **codomain**. We then write $f : A \to B$. For an element $a \in A$ the element $f(a) \in B$ is called the image of a.

There are many ways to represent functions. If the domain A is finite, we can list the images $f(a)$ for each element $a \in A$. This can be done with a table with a column for the inputs and another next to it that lists the corresponding outputs.

We can also represent the sets with bubbles and their elements with points and draw an arrow from every element in A to its corresponding image in B.

Functions can sometimes be given by explicit rules. When both the domain and codomain are sets of numbers, these rules can often be written with equations. When both the domain and codomain are the real line, the functions can be represented with their graphs in the plane, as you saw in Calculus classes.

Example 6.2. (a) Take as domain the set $A = \{a, b, c\}$, as codomain to the set of natural numbers and as assignment $f(a) = 1, f(b) = 1, f(c) = 3$. This assignment gives a function because each of the three elements in A has a well determined unique image which is a natural number.

With the same domain and codomain, the assignment $f(a) = 1, f(a) = 2, f(b) = 3, f(c) = 3$ does not give a function because a has two images.

With the same domain and codomain, the assignment $f(a) = 1, f(b) = 3$ does not give a function because c has no images.

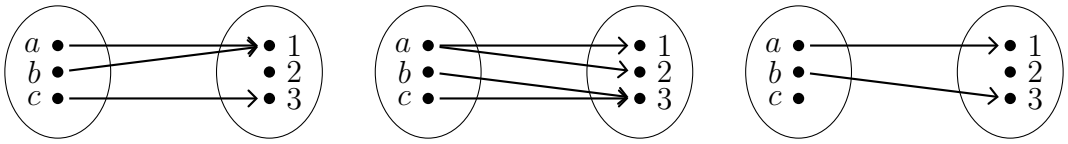


Figure 6. The first sketch is a function. The second is not because two arrows come out of a. The third is not because no arrow comes out of c.

(b) If $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ is a function as we assign to every real number a unique real number.

(c) If $f : \mathbb{R} \to \mathbb{R}^{\geq 0}$ given by $f(x) = x^2$ is a function as we assign to every real number a unique non-negative real number. This function is different from the previous one. Both have the same domain and rule but the codomains are different.

When giving a function with a rule, It is important to make sure that the rule makes sense. Sometimes an expression is not defined for some values of the intended domain, as when trying to divide by 0 or taking the square root of a negative real number. Another problem that it is often overlooked is that when we list the elements in the domain, they can be listed in several ways and the assignment rule would give different outputs depending on what representation you choose. Examples (a), (b), and (c) below may clarify what we mean:

Example 6.3. (a) In an elementary school, assign to each classroom the color of the T-shirt of a kid in that class on the first day of school. If we do not specify the child this would not give a well defined function if different kids in the same classroom wear T-shirst of different colors.

(b) The assignment $f : \mathbb{Q} \to \mathbb{Z}$ given by $f(\frac{m}{n}) = m$ is not a well defined function as 0.5 is a rational number that can be represented by $\frac{1}{2}, \frac{2}{4}, \frac{-3}{-6} \dots$ and we do not know if $f(.5)$ should be $1, 2, -3 \dots$

(c) The assignment $f : \mathbb{Q} \to \mathbb{Q}$ given by $f(\frac{m}{n}) = \frac{2m}{5n}$ is a well defined function. We need to check that the definition is independent of the way we represent a rational number as a fraction. Assume $\frac{a}{b} = \frac{c}{d}$. By definition, this implies $ad = bc$. Multiplying both sides of this equality by 10, we can write this as $(2a)(5d) = (5b)(2c)$ which tells us that $\frac{2a}{5b} = \frac{2c}{5d}$. So our assignment is not ambiguous and we get a well defined function from the rationa numbers to itself

(d) The assignment $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = \sqrt{x}$ is not a function as the image of the negative numbers is not well defined.

(e) The assignment $f : \mathbb{C} \to \mathbb{C}$ given by $f(x) = \sqrt{x}$ is not a well defined function as every complex number (except for 0) has two square roots (please check it). Unlike the real case, we cannot choose " the positive root". For example, the two square roots of $-i$ are $-\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i, \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i$. None of them seems more "positive" than the other.

Definition 6.4. Given a function $f : A \to B$ and a function $g : B \to C$, the **composition** of the two functions f, g is a function $g \circ f : A \to C$ given by the rule $(g \circ f)(a) = g(f(a)), \forall a \in A$.

Note in particular that we can only compose two functions if the codomain of the first is the domain of the second. Then, the composition is obtained by doing the two functions one after the other.

Example 6.5. (a) A first example is given in picture 7.

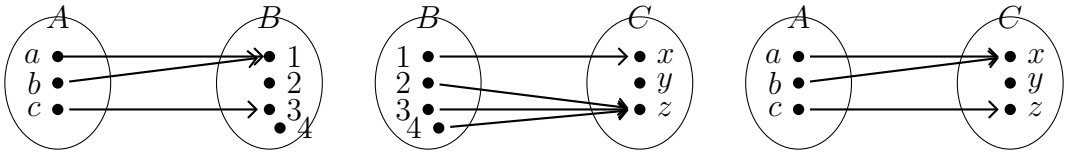


FIGURE 7. The functions f, g and their composition $g \circ f$.

(b) Consider the two functions $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x + 2$ and $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = 3x$. In this case, as the domain and codomain are the same, it makes sense to compose the two functions in any order.

$$(f \circ g)(x) = f(g(x)) = f(3x) = 3x + 2, \quad (g \circ f)(x) = g(f(x)) = g(x + 2) = 3(x + 2) = 3x + 6$$

We see that in the rare cases in which it makes sense to compose functions in both orders, the composition is not commutative

Definition 6.6. Given a function $f : A \to B$, the **image** or **range** of f is the subset of B consisting of images of elements in A

$$Im\ f = \{b \in B | \exists a \in A \text{ such that } f(a) = b\}.$$

Given a subset $A_1 \subseteq A$, the image of A_1 is defined similarly as the collection of images of elements in A.

$$f(A_1) = \{b \in B | \exists a \in A_1 \text{ such that } f(a) = b\}.$$

Given a subset of B, $B_1 \subseteq B$, its **inverse image** $f^{-1}(B_1)$ are the elements in A that map to B_1:

$$f^{-1}(B_1) = \{a \in A \mid f(a) \in B_1\}.$$

Example 6.7. (a) Consider the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$. The image or range of this function is the set of non-negative real numbers.

If we take the open interval in the real line $(-2, 2) = A_1$, then its image is the half closed interval $f(A_1) = (0, 4)$. Computing the inverse images of some sets, we have $f^{-1}(\{4\}) = \{2, -2\}$, $f^{-1}(\{-4\}) = \emptyset$.

Definition 6.8. A function $f : A \to B$ is **one to one** or **injective** if $a_1 \neq a_2$ implies $f(a_1) \neq f(a_2)$.

We normally check that f is one to one by assuming that $f(a_1) = f(a_2)$ and showing that this implies $a_1 = a_2$.

A function $f : A \to B$ is **onto** or **surjective** if $\forall b \in B, \exists a \in A$ with $f(a) = b$.

In plain english, a function is one to one if different elements map to different images. It is onto if every element in the codomain is the image of something in the domain.

Example 6.9. (a) The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ is neither one to one, nor onto: as $f(2) = f(-2)$, f cannot be one to one. As -4 is not in the image, f is not onto.

(b) Consider the function $\begin{array}{rccc} f & : & \mathbb{Z} & \to & \mathbb{Z} \\ & & z & \to & 3z+2 \end{array}$. Let us show that f is one to one. The condition for being one to one is that if $a_1 \neq a_2$ are two elements in the domain, then $f(a_1) \neq f(a_2)$. The easiest way to prove this is usually the contrapositive, assume $f(a_1) = f(a_2)$ and show then that $a_1 = a_2$.

Assume that $a_1, a_2 \in \mathbb{Z}$ and $f(a_1) = f(a_2)$. From the definition of f, we obtain, $3a_1 + 2 = 3a_1 + 2$. Subtracting 2 from both sides of the equation and dividing by 3, $a_1 = a_2$, showing that f is one to one..

Let us show that f is not onto because some integers are not in the image: assume $f(a) = 1$. Then $3a + 2 = 1$ which gives $3a = -1$. This equation says that -1 is divisible by 3, which is false. Hence-1 cannot be written as $f(a)$ for any $a \in \mathbb{Z}$. By definition of onto, f is not onto.

(c) Consider the function $\begin{array}{rccc} f & : & \mathbb{R} & \to & \mathbb{R} \\ & & r & \to & 3r+2 \end{array}$ The same proof we gave in (b) shows that this new f is also one to one. Moreover, this function f is onto: given $x \in \mathbb{R}$, $f(\frac{x-2}{3}) = 3(\frac{x-2}{3}) + 2 = x$. Hence, every $x \in \mathbb{R}$ is in the image of f which is the definition of onto.

7. Bijections, Sept 29.

Let us look at functions that are both one to one and onto We start by defining the type of functions that allow us to identify two sets:

Definition 7.1. A function $f : A \to B$ is **a bijection** if it is both one to one and onto. Equivalently, $\forall b \in B, \exists! a \in A$ with $f(a) = b$.

In plain english, a function is a bijection if every element in the codomain is the image of one and only one element in the domain.

Example 7.2. (a) For any set A, the identity function $I_A : A \to A$ given by $I_A(x) = x$ is one to one and onto, hence a bijection.

(b) The function $\begin{array}{rccc} f & : & \mathbb{R} & \to & \mathbb{R} \\ & & x & \to & 3x+2 \end{array}$ is a bijection as shown in Example 6.9.

A characterization of bijections is that the functions can be "undone" with another function:

Theorem 7.3. *If a function $f : A \to B$ is one to one and onto, then there exists a function $g : B \to A$ such that $f \circ g = I_B, g \circ f = I_A$ Conversely if there exists $g : B \to A$ such that $f \circ g = I_B, g \circ f = I_A$, then f is a bijection.*

Proof. The main idea is that if f is a bijection, there is a natural way of choosing for each element in B one in A that allows you to go back.

Assume that f is a bijection. Define $g : B \to A$ as follows: as f is onto, for every $b \in B$, there exists $a \in A$, $f(a) = b$. As f is one to one, this a is unique. Hence, we can define $g(b) = a$ and this a is determined uniquely in an unambigous way. As, by assumption, $f(a) = b$, it follows that $f(g(b)) = f(a) = b, \forall b \in B$. Equivalently, $f \circ g = I_B$. Also, with the above notations, $\forall a \in A$, $g(f(a)) = g(b) = a$. Hence, $g \circ f = I_A$.

Let us now prove the converse. Assume that there exists a $g : B \to A$ such that such that $f \circ g = I_B, g \circ f = I_A$. For any $b \in B$, $f(g(b)) = b$, so f is onto. Assume $f(a_1) = f(a_2)$. Then $a_1 = g(f(a_1)) = g(f(a_2)) = a_2$. Hence, f is one to one. □

Example 7.4. (a) For the identity function $I_A : A \to A$ given by $I_A(x) = x$ the corresponding g from the Theorem above is again $g = I_A$.

(b) For the function $\begin{array}{rccc} f & : & \mathbb{R} & \to & \mathbb{R} \\ & & r & \to & 3r+2 \end{array}$ the corresponding g is given as $g(x) = \frac{x-2}{3}$. Let us check that this works:

$$(f \circ g)(x) = f(\frac{x-2}{3}) = 3\frac{x-2}{3} + 2 = x, \quad (g \circ f)(x) = g(3x+2) = \frac{(3x+2)-2}{3} = \frac{3x}{3} = x$$

as needed.

An important observation is that in the above Theorem, you need the two conditions $f \circ g = I_B, g \circ f = I_A$ for f to be a bijection. One of them only would not be enough. For example, denote by $\mathbb{R}^+$ the real numbers greater than or equal to 0. Define $f : \mathbb{R} \to \mathbb{R}^+, g : \mathbb{R}^+ \to \mathbb{R}$ by $f(x) = x^2, g(x) = \sqrt{x}$. Then $f \circ g = I_{\mathbb{R}^+}$ but neither f nor g are bijections.

Proposition 7.5. *Assume that $f : A \to B$ is any function. Let $B_1 \subseteq B$ be any subset of B. Recall that we defined the inverse image of a set by an arbitrary function as*

$$f^{-1}(B_1) = \{a \in A \mid f(a) \in B_1\}.$$

Assume now that f is a bijection and that $g : B \to A$ is the function satisfying $f \circ g = I_B, g \circ f = I_A$.. Then, $f^{-1}(B_1) = g(B_1)$.

Proof. We need to prove the two inclusions We start with $f^{-1}(B_1) \subseteq g(B_1)$: take $a \in f^{-1}(B_1)$. By definition of $f^{-1}(B_1)$, $f(a) = b \in B_1$. By definition of g, $g(b) = a$. Hence $a \in g(B_1)$. As this is true for every $a \in f^{-1}(B_1)$, we conclude that $f^{-1}(B_1) \subseteq g(B_1)$.

Take now $a \in g(B_1)$. By definition of image of a set, there exists $b \in B_1$ such that $a = g(b)$. By definition of g, this means that $f(a) = b$. Hence, $f(a) \in B_1$. By definition of inverse image, this means that $a \in f^{-1}(B_1)$. As this is true for every $a \in g(B_1)$, we conclude that $g(B_1) \subseteq f^{-1}(B_1)$. □

Definition 7.6. Let $f : A \to B$ be a bijection. Then, the function $g : B \to A$ such that $f \circ g = I_B, g \circ f = I_A$ is called the inverse of f and is written as $g = f^{-1}$.

Proposition 7.7. *Let A, B, C be three sets, f, g functions $f : A \to B,\ g : B \to C,\ h = g \circ f : A \to C$ Prove thzt if f, g are bijections, then h is a bijection.*

Proof. Assume that both f, g are bijections with inverses $\bar{f}, \bar{g}$. This means that

$$\bar{f} \circ f = I_A, f \circ \bar{f} = I_B,\ \bar{g} \circ g = I_B, g \circ \bar{g} = I_C$$

We claim that $\bar{h} = \bar{f} \circ \bar{g} : C \to A$ is the inverse of $h = g \circ f : A \to C$. It suffices to check that the composition in either order gives the identity in the corresponding set. We find

$$h \circ \bar{h} = (g \circ f) \circ (\bar{f} \circ \bar{g}) = g \circ (f \circ \bar{f}) \circ \bar{g} = g \circ I_B \circ \bar{g} = g \circ \bar{g} = I_C$$

$$\bar{h} \circ h = (\bar{f} \circ \bar{g}) \circ (g \circ f) = \bar{f} \circ (\bar{g} \circ g) \circ f = \bar{f} \circ (I_C) \circ f = \bar{f} \circ f = I_A$$

□

8. Cardinality, Oct 4.

In this sections we want to look at the question of whether two sets can be identified and in particular at whether they have the same number of elements. We will see that the concept "having the same number of elements" makes sense not only for finite sets but also for infinite ones.

Over the years, we have all developed some intuition for the concepts of "more", "less" and "the same" based on our experience with finite sets. For infinite sets, the answers to some questions may be different from what we would expect from this intuition. For a start, with our definition, it will not be true that all infinite sets have the same number of elements. On the other hand, while the set of integers strictly contains the set of natural number and the set of rational numbers strictly contains the integers, we will see that all these sets have the same number of elements. The real numbers on the other hand have many more elements. Let us start with a definition:

Definition 8.1. We say that two sets A, B have the same **cardinality** if and only if there is a bijection between the two. We then write $|A| = |B|$.

We say that a set A is **finite of cardinality** n if there is a bijection between A and the set A_n with $A_0 = \emptyset,\ A_n = \{1, 2, \dots, n\}, n \geq 1,\ n \in \mathbb{N}$. We then say that $|A| = n$. In particular, $|\emptyset| = 0$.

We say that a set is **infinite** if it is not finite.

Example 8.2. (a) The set the set $B_n = \{0, 1, 2, \dots, n-1\}$ is finite of cardinality n. We can prove this by establishing a bijection between this set and the set $A_n = \{1, 2, \dots, n\}$. We can define the maps

$$\begin{array}{cccc} f_n: & A_n & \to & B_n \\ & a & \to & a-1\text{'} \end{array} \qquad \begin{array}{cccc} g_n: & B_n & \to & A_n \\ & b & \to & b+1 \end{array}$$

First, these two maps are well defined. If $a \in A_n$, it means that a is a natural number with $1 \leq a \leq n$. Then $a-1$ is a natural number with $0 \leq a \leq n-1$. Similarly, if $b \in B_n$, it means that b is a natural number with $0 \leq b \leq n-1$. Then $b+1$ is a natural number with $1 \leq a \leq n$. The two functions are inverse of each other

$$g_n \circ f_n(a) = g_n(f_n(a)) = g_n(a-1) = (a-1)+1 = a, \quad f_n \circ g_n(b) = f_n(g_n(b)) = f_n(b+1) = (b+1)-1 = b$$

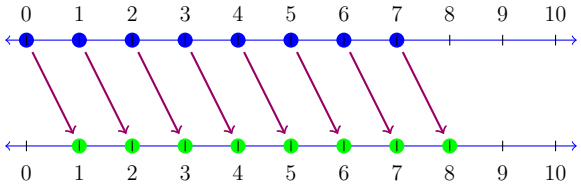


Figure 8. The bijection between B_8 (in blue) and A_8 (in green).

(b) If $j \in A_n = \{1, 2, \dots, n\}$, then $A_n - \{j\}$ is finite of cardinality $n-1$. To prove the result, we need to establish a bijection between $A_n - \{j\}$ and A_{n-1}. We can do this by shifting down by one all the numbers larger than j in $A_n - \{j\}$ or by increasing by one all the numbers greater than or equal to j in A_{n-1}. If we want to write the bijections explicitly,

we can do so as follows $f : A_n - \{j\} \to A_{n-1},\ g : A_{n-1} \to A_n - \{j\}$

$$f(m) = \begin{cases} m & \text{if } m < j \\ m-1 & \text{if } m > j \end{cases} \qquad g(k) = \begin{cases} k & \text{if } k < j \\ k+1 & \text{if } k \geq j \end{cases}$$

The we can check that both f and g are well defined as the image of f gives natural numbers smaller than n and the image of g does not contain j. Moreover, you can check that they are inverses of each other and therefore bijections.

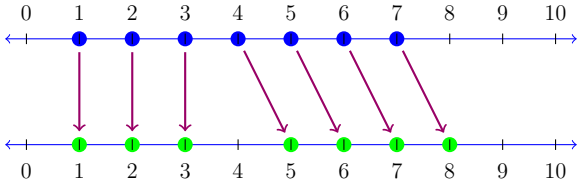


FIGURE 9. The bijection between A_7 (in blue) and $A_8 - \{4\}$ (in green).

We need to check that the cardinality of a set is well defined. By this we mean that there cannot be a set with cardinality n and at the same time cardinality m unless $m = n$. If this were to happen, there would be a bijection between A_n and A_m. Let us see that this is not possible:

Proposition 8.3. *Assume there is a bijection between A_n and A_m. Then, $m = n$.*

Proof. We can assume $n \leq m$ and prove the result by induction on n. If $n = 0$, then $A_n = \emptyset$. This implies that also $A_m = \emptyset$, otherwise, the elements of A_m would have nowhere to go by a bijection with A_n.

Assume now that the result is true up to n and prove it for A_{n+1}. Assume there is a bijection $f : A_{n+1} \to A_m$. There is then also a bijection

$$\bar{f} : A_n = A_{n+1} - \{n+1\} \to A_m - \{f(n+1)\} \text{ defined by } \bar{f}(x) = f(x).$$

As f is one to one, no other number but n maps to $f(n)$. Hence, $\bar{f}$ is well defined. Also, $\bar{f}$ is one to one as it is the restriction of f that is one to one. Moreover, $\bar{f}$ is onto: given $y \in A_m - \{f(n+1)\}$, as f is onto, there exists $x \in A_{n+1}$ such that $f(x) = y$. As $y \neq f(n+1)$ and f is one to one, $x \neq n+1$. Hence, $x \in A_n$ and $\bar{f}(x) = y$.

From Example 8.2 (b), there is a bijection from $A_m - \{f(n+1)\}$ to A_{m-1}. Composing with $\bar{f}$, we obtain a bijection between A_n and A_{m-1}. By the induction assumption, $n = m - 1$ and therefore, $n + 1 = m$ as we had to prove. □

Proposition 8.4. *If A is a finite set with n elements and $B \subseteq A$, then B is a finite set with at most n elements and it has precisely n elements if and only if $B = A$.*

Proof. As A is finite with n elements, there is a bijection between A and $A_n = \{1, 2, \ldots, n\}$. Using this bijection, we can identify A with A_n and just assume that B is a subset of A_n. What we need to do is define a bijection between B and a set $A_k = \{1, 2, \ldots, k\}$, for some $k \leq n$. Equivalently, we need to label the elements of B with numbers $1, 2, \ldots, k$ for some k We can do this as follows: we choose the smallest element $b_1 \in B$ and we will label it with 1, then we choose the smallest number in $b_2 \in B - \{b_1\}$ and we label it with 2 and so on. We keep going until we run out of elements in B. As $a_1 \in B \subseteq A_n = \{1, 2, \ldots, n\}$,

$1 \leq b_1$. From our choice of b_1 as the smallest element B , $1 \leq b_1 < b_2$, so $2 \leq b_2$. Similarly $j \leq b_j$ and because all the elements in B are in A_n, they are all at most n. So, we will run out of elements in B after at most n steps. Moreover, if we need all of the n steps, then $b_1 = 1, b_2 = 2, \ldots, b_n = n$ and therefore $B = A_n$. □

Definition 8.5. We say that a set A is **countable** if there is a bijection between A and the set of natural numbers $\mathbb{N}$.

Example 8.6. (a) The set of even natural numbers is countable. By definition, a natural number a is even if there exists another natural number b such that $a = 2b$. We can define functions from the set of natural numbers to the set E of even numbers and back by

$$\begin{array}{rccc} f: & \mathbb{N} & \to & E \\ & a & \to & 2a \end{array} \qquad \begin{array}{rccc} g: & E & \to & \mathbb{N} \\ & b & \to & \frac{b}{2} \end{array}$$

These functions are well defined as by definition, a natural number b is even if and only if there exists another natural number a such that $b = 2a$. So, for any natural number a, $2a$ is an even number and for every even number b, $\frac{b}{2}$ is a natural number. Moreover, the two functions are inverse of each other as

$$g \circ f(a) = g(f(a)) = g(2a) = \frac{2a}{2} = a, \quad f \circ g(b) = f(g(b)) = f(\frac{b}{2}) = 2\frac{b}{2} = b$$

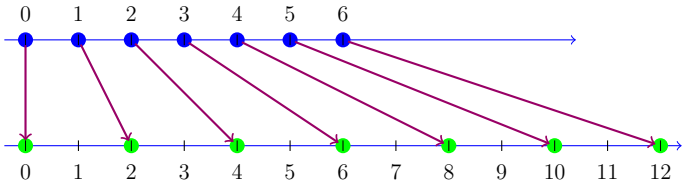


FIGURE 10. The bijection between the natural and even numbers.

(b) The set of integers is countable. We can give bijections between the natural numbers by making the even natural numbers correspond to the positive integers and the odd natural numbers to the negatives. We. can define functions explicitly as follows: Define $f : \mathbb{N} \to \mathbb{Z}$ and $g : \mathbb{Z} \to \mathbb{N}$ as follows :

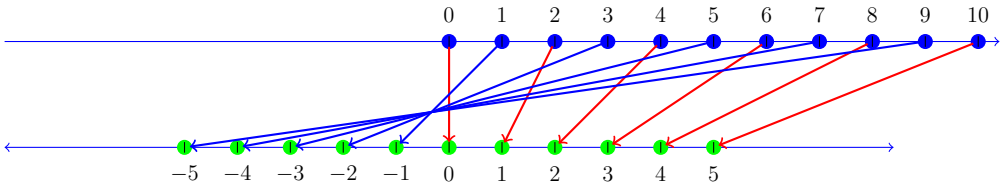


FIGURE 11. The bijection between the natural numbers and the integers.

$$f(m) = \begin{cases} \frac{m}{2} & \text{if } m \text{ even} \\ -\frac{m+1}{2} & \text{if } m \text{ odd} \end{cases} \qquad g(z) = \begin{cases} 2z & \text{if } z \geq 0 \\ -2z-1 & \text{if } z < 0 \end{cases}$$

Note that f is a well defined function: if m is even, $\frac{m}{2}$ is even. If m is odd, then $m+1$ is even and $-\frac{m+1}{2}$ is a well defined (negative) integer. Also g is a well defined integer: if

$z \geq 0$ then $2z$ is a natural number. If $z < 0$, then $z \leq -1$ and $-2z - 1 \geq 2 - 1 = 1$ is a natural number. We now check that f, g are inverse of each other. This will suffice to ensure they are both bijections.

$$g(f(m)) = \begin{cases} g(\frac{m}{2}) = 2\frac{m}{2} = m & \text{if } m \text{ even} \\ g(-\frac{m+1}{2}) = -2(-\frac{m+1}{2}) - 1 = m & \text{if } m \text{ odd} \end{cases}$$

$$f(g(z)) = \begin{cases} f(2z) = z & \text{if } z \geq 0 \\ f(-2z-1) = -\frac{(-2z-1)+1}{2} = z & \text{if } z < 0 \end{cases}$$

Proposition 8.7. *If A is a countable set and $B \subseteq A$, then B is either finite or countable*

Proof. As A is countable, there is a bijection between A and $\mathbb{N}$. Using this bijection, we can identify A with $\mathbb{N}$ and just assume that B is a subset of $\mathbb{N}$.

What we need to do is to find a way to label the elements in B as $1, 2, \ldots, k, \ldots$. We proceed as in the case of a subset of a finite set: As B is a subset of $\mathbb{N}$, from the well ordering principle, we choose the smallest element $b_1 \in B$ and we will label it with 1. Next, we choose the smallest number in $b_2 \in B - \{b_1\}$ and we label it with 2 and so on. We keep going. If we run out of elements in B after n steps, then B is finite of cardinality n. If we never run out, then B is countable. □

Proposition 8.8. *The set of positive rational numbers is countable.*

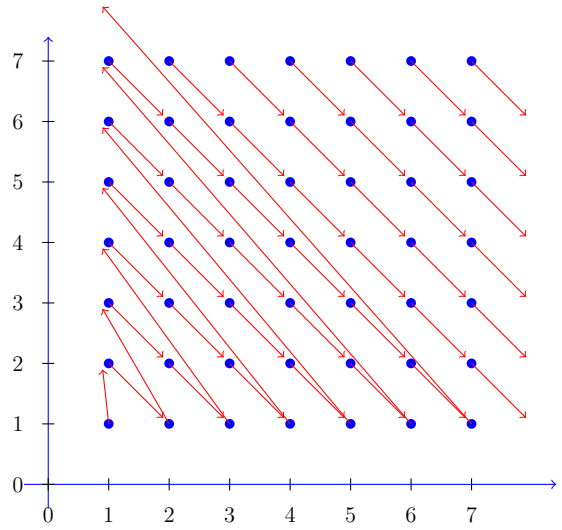


FIGURE 12. Enumeratinng positive fractions, or more concretely, pairs of rational integers.

Proof. Every positive rational number can be represented in a unique way as a quotient of two positive numbers with no common factors. The set of positive fractions in lowest terms is a subset of the set of all fractions such that the numerator and denominator are both positive. As an infinite subset of a countable set is also countable, we only need to show that the set of all fractions such that the numerator and denominator are both positive is countable. Equivalently, we need to show that the set of pairs of positive natural numbers

is countable. We can order them in increasing order by their sum and within each sum in increasing order by the first term, so

$$(a,b) \leq (c,d) \iff a+b < c+d \text{ or } [a+b = c+d \text{ and } a \leq c]$$

We would get a list such as

$$(1,1),(1,2),(2,1),(1,3),(2,2),(3,1),(1,4),(2,4),(3,4),(4,4),(1,5)\ldots$$

The explicit expressions from the set P of pairs of strictly positive integers to the set of natural numbers is rather complicated, so you can skip the rest of this proof if you wish. If you actually want to give this expression , we fist need to figure out how many pairs add to a given value. The pairs (a,b) with $a+b=n$ are $(1,n-1),(2,n-2),\ldots,(n-1,1)$. There are $n-1$ such pairs. Therefore, before the pair (a,b) there are 1 pair that adds up to 2, 2 pairs that add up to 3,..., $a+b-2$ pairs that add up to $a+b-1$ and a pairs (including (a,b)) that add up to $(a+b)$ and have first components at most a. Therefore, the place for (a,b) in the line is

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

if we start counting at 0. That is, the bijection is given by

$$\begin{array}{rccc} f: & P & \to & \mathbb{N} \\ & (a,b) & \to & \frac{(a+b-1)(a+b-2)}{2}+a-1 \end{array}$$

To define the map the other way around, notice that the expressions $\frac{(n-1)(n-2)}{2}$ is an increasing function of n that is unbounded. Given an arbitrary natural number m, we can find a unique value of n such that)

$$\frac{(n-1)(n-2)}{2} < m+1 \leq \frac{n(n-1)}{2}$$

Then, we define the inverse function as follows:

$$\begin{array}{rccc} g: & \mathbb{N} & \to & P \\ & m & \to & (m+1-\frac{(n-1)(n-2)}{2}, n-m-1+\frac{(n-1)(n-2)}{2}) \end{array}$$

□

Theorem 8.9. *The set of rational numbers is countable.*

Proof. As the positive rationals are countable, there is a bijection between the positive rationals and $\mathbb{N}$. There is a bijection between the positive rational and the negative rationals, therefore, a bijection between the negative rationals and $\mathbb{N}$. If we add 0 to the positive rationals, this is still in bijection with $\mathbb{N}$, we just need to slide numbers up and down to get a bijection or its inverses. Then, as in the proof that the integers form a countable set, we can construct a bijection between the rational numbers and $\mathbb{N}$, by assigning the positive or 0 rationals to the even natural numbers and the negative rationals to the odd natural numbers. □

Theorem 8.10. *The set of real numbers is not countable.*

Proof. In the homework, you will show that there is a bijection between the real line and any open interval. If the real line were countable, then the interval $(0, 1)$ would also be countable. The interval $(0, 1)$ consists of all the decimals expressions between 0 and 1 where the decimals may or may not repeat. Let us show that the interval $(0, 1)$ is not countable.

If the interval $(0, 1)$ were countable, we could order all the decimals expressions between 0 and 1 and put them in correspondence with the numbers 1, 2, 3, ... Let us show that there is one decimal between 0 and 1 not in our list: to define the digit in the n^{th} spot of our new decimal, we look at the digit in the n^{th} spot of the n^{th} decimal in our list. If that digit is $a < 9$, in our new decimal we place $a + 1$ in the n^{th} spot. If that digit is $a = 9$, in our new decimal we place 0 in the n^{th} spot. For example, if our list starts as

$$\begin{array}{cc} 1 & 0.123123123\ldots \\ 2 & 0.121221222\ldots \\ 3 & 0.123456789\ldots \\ 4 & 0.345189237\ldots \\ 5 & 0.116722298\ldots \\ 6 & 0.336721498\ldots \\ 7 & 0.000999835\ldots \\ \ldots & \ldots \end{array}$$

our new decimal would start as $0.2342320\ldots$.

The new decimal we constructed is different from all the ones we had before as it differs from each of them in at least one spot. Also, it is strictly between 0 and 1:if it were identically 0, it would mean that in the original list, the n^{th} number had the digit 9 on the n^{th} spot. But many decimals between 0 and 1have no 9's at all, so the original list was incomplete. Similarly, if the new number were $0.999999\cdots = 1$, it would mean that in the original list the n^{th} number had the digit 0 on the n^{th} spot. But many decimals between 0 and 1 have no 0's at all, so the original list was incomplete. This completes the proof that the interval of the real line $(0, 1)$ is not countable and therefore $\mathbb{R}$ itself is not countable. □

9. Counting problems, union of sets, October 6

Proposition 9.1. *Assume that A, B are finite, disjoint (that is, $A \cap B = \emptyset$) sets with m and n elements respectively. Then $A \cup B$ is finite of cardinality $m + n$.*

Proof. From our assumptions, there exist bijections

$$f : A \to \{1, \dots, m\},\ g : B \to \{1, \dots, n\}$$

We construct a bijection $h : A \cup B \to \{1, \dots, m + n\}$ as follows

$$h(x) = \begin{cases} f(x) & \text{if } x \in A \\ g(x) + m & \text{if } x \in B \end{cases}$$

We show that h is one to one: assume that $h(x_1) = h(x_2)$. If $x_1, x_2 \in A$, then $f(x_1) = h(x_1) = h(x_2) = f(x_2)$. As f is one to one, this implies $x_1 = x_2$. If $x_1, x_2 \in B$, then $g(x_1) + m = h(x_1) = h(x_2) = g(x_2) + m$. Then also $g(x_1) = g(x_2)$. As g is one to one, this implies $x_1 = x_2$. If $x_1 \in A,\ x_2 \in B$, then $h(x_1) = f(x_1) \leq m,\ h(x_2) = g(x_2) + m \geq m + 1$. Hence, it is impossible to have $h(x_1) = h(x_2)$.

The map h is onto: Choose $y \in \{1, \dots, m + n\}$. If $y \leq m$, as f is onto, there exists $x \in A$ such that $f(x) = y$. As $f(x) = h(x)$, then $h(x) = y$. If $m + 1 \leq y \leq m + n$, then $1 \leq y - m \leq n$. As g is onto, there exists $x \in B$ such that $g(x) = y - m$. As $h(x) = g(x) + m = (y - m) + m = y$, then $h(x) = y$. Hence, h is onto. Then h leads to an explicitly bijection between the set $A \cup B$ and the set $\{1, \dots, m + n\}$. Therefore, $|A \cup B| = m + n$ □

Proposition 9.2. *Assume that A, B are finite sets. Then $A \cup B$ is finite and*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Proof. We can write B as the union of two disjoint sets

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

Using Proposition 9.1, $|B| = |B - A| + |A \cap B|$. Equivalently, $|B - A| = |B| - |A \cap B|$.

We can write $A \cup B$ as the union of two disjoint sets

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

Using again Proposition 9.1 and the result above,

$$|A \cup B| = |A| + |B - A| = |A| + |B| - |A \cap B|$$

□

Proposition 9.3. *Assume that $A_1 \dots, A_n$ are finite sets. Then $A_1 \cup \dots \cup A_n$ is finite and*

$$|A_1 \cup \dots \cup A_n| = \Sigma_{i=1}^n |A|_i - \Sigma_{i \neq j} |A_i \cap A_j| + \Sigma |A_i \cap A_j \cap A_k| + \dots + (-1)^{n-1} |A_1 \cap \dots \cap A_n|$$

Proof. We can use induction on n. Let us just do the case of $n = 3$ as an illustration.

We can write $A_1 \cup A_2 \cup A_3$ as the union of two sets, one being $A = A_1 \cup A_2$ and the other being $B = A_3$. Using the result that we know for two sets,

$$(*)\ \ |A \cup B| = |A| + |B| - |A \cap B| = |A_1 \cup A_2| + |A_3| - |(A_1 \cup A_2) \cap A_3|$$

We can apply again the rule for the union of two sets to $A_1 \cup A_2$ and get that

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

We can rewrite $(A_1 \cup A_2) \cap A_3$ as a union of two sets as $(A_1 \cap A_3) \cup (A_2 \cap A_3)$. Then, apply again the rule for the union of two sets to $A = A_1 \cap A_3,\ B = A_2 \cap A_3$.

$$|(A_1 \cap A_3) \cup (A_2 \cap A_3)| = |A_1 \cap A_3| + |A_2 \cap A_3| - |(A_1 \cap A_3) \cap (A_2 \cap A_3)|$$

Now, $(A_1 \cap A_3) \cap (A_2 \cap A_3) = A_1 \cap A_2 \cap A_3$. Substitute now the values of the equations above in (*) to obtain

$$|A_1 \cup A_2 \cup A_3| = |A_1 \cup A_2| + |A_3| - |(A_1 \cup A_2) \cap A_3| =$$
$$= |A_1| + |A_2| - |A_1 \cap A_2| + |A_3| - [|A_1 \cap A_3| + |A_2 \cap A_3| - |(A_1 \cap A_2 \cap A_3|] =$$
$$= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

□

Example 9.4. (a) In a survey of 300 democratic leaning voters, 45 were young voters ages 18-25,103 identified as latinex including 27 young latinex, 162 identified as women including 59 latinas. How many young latinas were in the group?

Let us formulate the question as follows: Let A_1 be the set of latinex voters, A_2 the set of young voters and A_3 be the set of women. We have the following data

$$|A_1 \cup A_2 \cup A_3| = 300,\ |A_1| = 103,\ |A_2| = 45,\ |A_3| = 162, |A_1 \cap A_2| = 27, |A_2 \cap A_3| = 59$$

We are being asked about the cardinality $|A_1 \cap A_2 \cap A_3|$. We do not have enough data to determine this number as we do not know the number of young women $|A_2 \cap A_3|$. Knowing either of these numbers would allow us to determine the other using the equation in Proposition 9.3

(b) In a survey of 500 household, all of them plan to buy something special for Halloween. A full 387 plan on buying candy, 153 will buy decorations and 147 will buy costumes. If only 64 will buy all three, how many will buy precisely two of the three things?

Let us formulate the question as follows: Let A_1 be the set of households buying candy, A_2 the set of households buying decorations and A_3 be the set of households buying costumes. We have the following data

$$|A_1 \cup A_2 \cup A_3| = 500,\ |A_1| = 387,\ |A_2| = 153,\ |A_3| = 147, |A_1 \cap A_2 \cap A_3| = 64$$

We are being asked about the cardinality $|(A_1 \cap A_2) \cup (A_1 \cap A_3) \cup |(A_2 \cap A_3) - (A_1 \cap A_2 \cap A_3)|$. Using the equation in Proposition 9.3, we have

$$500 = 387 + 153 + 147 - (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) + 64$$

This does not allow us to compute the individual values of $|A_1 \cap A_2|, |A_1 \cap A_3|, |A_2 \cap A_3|$ but we can compute their sum $|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3| = 251$. Note now that $A_1 \cap A_2 \cap A_3 \subseteq A_1 \cap A_2$ so we can write the sets as disjoint union

$$(A_1 \cap A_2) = [(A_1 \cap A_2) - (A_1 \cap A_2 \cap A_3)] \cup (A_1 \cap A_2 \cap A_3)$$

So, the number of elements of the set in the left is the sum of the number of elements of the two sets on the right and similarly with the other pairs. The set we are interested cann be written as the union of three disjoint sets as follows:

$$X = (A_1 \cap A_2) \cup (A_1 \cap A_3) \cup (A_2 \cap A_3) - (A_1 \cap A_2 \cap A_3) =$$
$$= [(A_1 \cap A_2) - (A_1 \cap A_2 \cap A_3)] \cup [(A_1 \cap A_3) - (A_1 \cap A_2 \cap A_3)] \cup [(A_2 \cap A_3) - (A_1 \cap A_2 \cap A_3)]$$

So, the number of elements of X is the sum of the number of elements of each of the three sets. Therefore,

$$|(A_1 \cap A_2) \cup (A_1 \cap A_3) \cup (A_2 \cap A_3) - (A_1 \cap A_2 \cap A_3)| = |A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3| - 3|A_1 \cap A_2 \cap A_3|$$

Therefore, there are $251 - 3 \times 64 = 69$ household who are planning to buy precisely two of the types of Halloween items.

10. Counting problems: products and factorials, October 18.

Recall that the cartesian product of two sets is the set of pairs with the first element in the first set, the second in the second set. We saw in the previous section that the disjoint union of two sets has cardinality equal to the sum of the two cardinalities. In a similar way, we are going to see now that the cartesian product has cardinality equal to the product of the two cardinalities

Proposition 10.1. *Assume that A, B are finite sets of cardinality m and n respectively. Then $A \times B$ is finite of cardinality mn.*

Proof. From our assumptions, there exist bijections

$$f : A \to \{1, \dots, m\},\ g : B \to \{1, \dots, n\}$$

We construct a bijection $h : A \times B \to \{1, \dots, mn\}$ as follows

$$h(a, b) = m(g(b) - 1) + f(a).$$

This h is well defined: as $1 \leq f(a) \leq m, 1 \leq g(b) \leq n$

$$1 = m(1 - 1) + 1 \leq m(g(b) - 1) + f(a) \leq m(n - 1) + m = mn$$

and therefore the image of h is in the given codomain.

We show that h is one to one: assume that

$$h(a_1, b_1) = h(a_2, b_2).$$

Equivalently,

$$h(a_1, b_1) = m(g(b_1) - 1) + f(a_1) = m(g(b_2) - 1) + f(a_2) = h(a_2, b_2).$$

As $1 \leq f(a_1) \leq m$, the remainder of dividing $h(a_1, b_1)$ by m is $f(a_1)$ if $f(a_1) < m$ and 0 if $f(a_1) = m$. For the same reason, using that also $1 \leq f(a_2) \leq m$, the remainder of dividing $h(a_1, b_1) = h(a_2, b_2)$ by m is $f(a_2)$ if $f(a_2) < m$ and 0 if $f(a_2) = m$. As this remainder is unique, $f(a_1) = f(a_2)$. As f is one to one, this implies $a_1 = a_2$. From $f(a_1) = f(a_2)$ and $h(a_1, b_1) = m(g(b_1)-1)+f(a_1) = m(g(b_2)-1)+f(a_2) = h(a_2, b_2)$, subtracting $f(a_1) = f(a_2)$ from both sides, $m(g(b_1) - 1) = m(g(b_2 - 1))$. Dividing both sides by m and adding 1, $g(b_1) = g(b_2)$. Then, as g is one to one, $b_1 = b_2$. Therefore, h is one to one.

Let us now check that h is onto. Given $y, 1 \leq y \leq mn$, we can divide y by m and get a unique quotient and unique remainder $y = qm + r,\ 0 \leq r < m$. If $r = 0$ as $y > 0$, this would imply that $q > 0$. Then, we can rewrite $y = (q - 1)m + 0$. So, in any case, we can write $y = q'm + r', 1 \leq r' \leq m$. Moreover, as $1 \leq y \leq mnn$, we need to have $0 \leq q' \leq n - 1$ As f is onto and $1 \leq r' \leq m$, there exists some $a \in A$ with $f(a) = r'$. As $0 \leq q' \leq n - 1$, then $1 \leq q' + 1 \leq n$. As g is onto, there exists some $b \in B$ such that $q' + 1 = g(b)$. Therefore,

$$y = q'm + r' = (g(b) - 1)m + f(a) = h(a, b)$$

Therefore, h is onto. Then h is a bjjection and $|A \times B| = mn$ □

Proposition 10.2. *Assume that $A_1 \dots, A_k$ are finite sets of cardinality $n_1 \dots, n_k$. Then the cartesian product $A_1 \times \cdots \times A_k$ is finite of cardinality $n_1 \dots n_k$.*

Proof. This can be proved by induction on k. We proved already the case $k = 2$.

Assume that the result is correct for $k-1$ and let us prove it for k. We assume then that the cardinality of $A_1 \times \cdots \times A_{k-1}$ is $n_1 \dots n_{k-1}$ Note that there is a bijection between the cartesian product $A_1 \times \cdots \times A_k$ and successive cartesian product of two sets

$$\begin{array}{rccc} f: & A_1 \times \cdots \times A_k & \to & (A_1 \times \cdots \times A_{k-1}) \times A_k \\ & (a_1, \dots, a_k) & \to & ((a_1, \dots, a_{k-1}), \dots, a_k) \end{array}$$

Using this bijection and using again the case of two sets,

$$|A_1 \times \cdots \times A_k| = |A_1 \times \cdots \times A_{k-1}||A_k| = (n_1 \dots n_{k-1})n_k = n_1 \dots n_k$$

Proving the equation for k. □

This counting method will be helpful when we try to enumerate events that are independent of each other:

Example 10.3. (a) In the presidential elections ballot in MA, you can vote for 1 of four presidential candidates or you can abstain. You can also vote yes, no or abstain to each of two ballot questions. Disregarding your choices in the rest of the ballot, which is likely to be linked to your choice for president, how many choices are there?

In this situation, your choice for president and the answer to the ballot questions are independent. There are 5 choices for president, including an abstention and three for each of the ballot questions. Hence, there are 45 possible outcomes.

(b) A partition of a set is a representation as a disjoint union of sets. If A is a set with n elements, let us find how many partitions there are of A with precisely two sets in the partition:

For each element in A, we need to decide if it will be in the first or second set. Hence, there are 2^n choices. Two of these choices are not allowed, namely all the elements are in the first set or all the elements are in the second set. This leaves us with $2^n - 2$ choices. Now, every partition will appear twice as the first and second set are not actually ordered. Hence, we need to divide the number of choices by 2. Therefore we have

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

Let us now see how to count certain choices that are not fully independent of each other:

Definition 10.4. Given a collection X of n distinct objects, a **permutation** of the objects is a way to order them from first to last. Equivalently, a permutation of X is a bijection from the set $A_n = \{1, 2, \dots, n\}$ to X.

Given a collection X of n distinct objects, a k**- permutation** of the objects is a way to choose k of them and order them from first to last. Equivalently, a k- permutation of X is a one to one function from the set $A_k = \{1, 2, \dots, k\}$ to X.

Definition 10.5. For any positive integer n we define n factorial as

$$n! = n(n-1)(n-2)\dots 3 \cdot 2 \cdot 1$$

We define

$$0! = 1$$

Proposition 10.6. *The number of permutations of n distinct objects is $n!$.*

The number of k permutation of n distinct objects is

$$n(n-1)\dots(n-k+1) = \frac{n!}{(n-k)!}.$$

Proof. If we want to define a bijection form the set $A_n = \{1, 2, \dots, n\}$ to X, we have n choices for the image of the first element, $n-1$ for the image of the second (as it cannot be the same as the image of the first element) and so on. For the last element, the image is the only element left in X that has not been chosen. Therefore, the total number of choices is $n!$.

The proof in the case of k-permutation is similar. □

Example 10.7. (a) With the three letters a, b, c, we can form, without repeating the letters, the following three letter words

$$abc, acb, bac, bca, cab, cba$$

(b) If we have 20 different toys, we can give them to 20 children in 20! different ways.

(c) If we have 9 identical balls, 6 identical hula hoops and 5 identical sleds, in how many ways can we give them to 20 children? If the toys were all different, we could give them to 20 children in 20! different ways. But reordering the toys of the same kind will not change the outcome. So, we can distribute the toys to the children in

$$\frac{20!}{9!6!5!}$$

different ways.

We have seen that the number of ordered k-tuples of a set with n elements is $n(n-1)\dots(n-k+1) = \frac{n!}{(n-k)!}$. Now we count the unordered ones

Definition 10.8. Given a set A with n elements and an integer k with $0 \leq k \leq n$, a k **combination** of A is a subset of A with k elements. The number of k combinations of A is denoted by $\binom{n}{k}$ ("n choose k").

Example 10.9. Let $A = \{a, b, c, d\}$. Then the combinations of A are

$$\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}$$

Therefore, $\binom{4}{2} = 6$.

Proposition 10.10. *The number $\binom{n}{k}$ of k combination of a set A with n elements is*

$$\binom{n}{k} = \frac{n(n-1)(n-2)\dots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$$

Proof. Recall that a k-permutation of n element is an ordered choice of k elements in a set of n. We already know that there are $n(n-1)(n-2)\dots(n-k+1)$ k-permutations of n elements. Any k permutation gives rise to a subset of k elements among the n. But a re-ordering of the k elements gives rise to the same subset. There are $k!$ reorderings of k elements. So, the number of k combinations is the number of k permutations divided by $k!$. □

Example 10.11. (a) To illustrate the proof of the proposition above with an example, the set of permutations of the set $A = \{a, b, c, d\}$ is given as

$$\{\{a,b\}\{a,c\},\{a,d\},\{b,a\},\{b,c\},\{b,d\},\{c,a\},\{c,b\},\{c,d\},\{d,a\},\{d,b\},\{d,c\}\}$$

There are two ways of reordering two elements ($2! = 2$). Therefore, every 2-permutation can be paired with another one giving rise to the same combination. In the above list, the two matching combinations are typed in the same color.

(b) The number of subsets with 3 elements of a set with 5 elements is

$$\binom{5}{3} = \frac{5 \times 4 \times 3}{3!} = \frac{5!}{3!2!} = \frac{5 \times 4}{2 \times 1} = 10$$

(c) The number of subsets with 2 elements of a set with 5 elements is

$$\binom{5}{2} = \frac{5!}{2!3!} = \frac{5 \times 4 \times 3}{3 \times .2 \times 1} = 10$$

This number is the same as the one above: choosing a subset with 3 elements of a set with five elements is equivalent to choosing its complement.

The identity we obtained in the last two examples can be generalized:

Proposition 10.12. *For any* $0 \leq k \leq n$,

$$\binom{n}{k} = \binom{n}{n-k}$$

Proof. We will give two different proofs of this result.

(a) First, an algebraic proof using the numerical definition of choose numbers:

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

(b) Now a combinatorial proof: the left hand side represents the number of subsets with k elements of a set with n elements. The right hand side represents the number of subsets with $n-k$ elements of a set with n elements. A subset with k elements determines a subset with $n-k$ elements as its complement and vice versa. Therefore, the two numbers are the same.

□

Proposition 10.13. *For any* $0 \leq k < n$,

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

Proof. We will give two different proofs of this result.

(a) First, an algebraic proof: We note first that

$$(n+1)! = (n+1) \times (n!), (k+1)! = (k+1) \times (k!), (n-k)! = (n-k) \times (n! - k - 1)!$$

Using the numerical definition of choose numbers, we can write the left hand side of the expression that we are trying to prove as

$$\binom{n}{k} + \binom{n}{k+1} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-k-1)!} =$$

$$n![\frac{k+1}{(k+1)!(n-k)!}+\frac{n-k}{(k+1)!(n-k)!}]=n!\frac{k+1+n-k}{(k+1)!(n-k)!}=\frac{(n+1)!}{(k+1)!(n-k)!}=\binom{n+1}{k+1}$$

(b) Now a combinatorial proof: The right hand side represents the number of subsets with $k+1$ elements of a set with $n+1$ elements that we write

$$A=\{a_1,\ldots,a_n,a_{n+1}\}=\{a_1,\ldots,a_n\}\cup\{a_{n+1}\}=A'\cup\{a_{n+1}\}$$

A subset of A with $k+1$ elements is either a subset of A' with $k+1$ elements or it is made of a subset of A' with k elements and the element a_{n+1}. There are $\binom{n}{k+1}$ subsets of the first kind and $\binom{n}{k}$ subsets of the second kind. Therefore, the sum of these two numbers is $\binom{n+1}{k+1}$.

□

In high school, you probably memorized the expansions

$$(a+b)^2=a^2+2ab+b^2,\ (a-b)^2=a^2-2ab+b^2$$

You proved them using the distributive property of product with respect to addition. What follows is a generalization of this equation for higher powers

Theorem 10.14. *[The binomial Theorem] Let a,b be real numbers, n a positive integer. Then*

$$(a+b)^n=\binom{n}{0}a^n+\binom{n}{1}a^{n-1}b+\binom{n}{2}a^{n-2}b^2+\cdots+\binom{n}{k}a^{n-k}b^k+\cdots+\binom{n}{n-1}ab^{n-1}+\binom{n}{n}b^n$$

Proof. We can again give two proofs. One is algebraic, using induction, the other is combinatorial.

(a) For the algebraic proof using induction:

- First step, check the case $n=1$:

$$(a+b)^1=\binom{1}{0}a^1+\binom{1}{1}b^1=a+b$$

holds true.

- Inductive step Assume that

$$(a+b)^n=\binom{n}{0}a^n+\binom{n}{1}a^{n-1}b+\cdots+\binom{n}{k}a^{n-k}b^k+\binom{n}{k+1}a^{n-k-1}b^{k+1}+\cdots+\binom{n}{n-1}ab^{n-1}+\binom{n}{n}b^n$$

Let us use this to compute $(a+b)^{n+1}=(a+b)^n(a+b)$ By the distributive property

$$(a+b)^n(a+b)=(a+b)^na+(a+b)^nb$$

Plugging in the value of $(a+b)^n$ that we assume correct by induction assumption, we obtain

$$(a+b)^{n+1}=$$

$$\begin{array}{ccccccccc}\binom{n}{0}a^{n+1}+&\binom{n}{1}a^nb+&\cdots+&\binom{n}{k}a^{n-k+1}b^k&+\binom{n}{k+1}a^{n-k}b^{k+1}&+\cdots+&\binom{n}{n}ab^n&+\\ +&\binom{n}{0}a^nb+&\cdots+&\binom{n}{k-1}a^{n-k+1}b^k&+\binom{n}{k}a^{n-k}b^{k+1}&+\cdots+&\binom{n}{n-1}ab^n&+\binom{n}{n}b^{n+1}\end{array}$$

Use now that

$$\binom{n}{0}=1=\binom{n+1}{0},\ \binom{n}{n}=1=\binom{n+1}{n+1},\ \binom{n}{k}+\binom{n}{k-1}=\binom{n+1}{k}$$

To write the above expression as

$$\binom{n+1}{0}a^{n+1}+\binom{n+1}{1}a^n b+\cdots+\binom{n+1}{k}a^{n-k+1}b^k+\binom{n+1}{k}a^{n-k}b^{k+1}+\cdots+\binom{n+1}{n}ab^n+\binom{n+1}{n+1}b^{n+1}$$

and this is the corresponding expression for $n+1$ instead of n.

(b) For a combinatorial proof: by definition of power of an expression

$$(a+b)^n=(a+b)(a+b)\dots(a+b)$$

Using the distributive property, this expression will be the sum of all possible products taking in the product an element of each of the parentheses. As there are n parentheses, each product will be the product of n terms. As the parentheses contain only a, b the resulting products will have expressions of the form $a^k b^{n-k}$. We need to count how many times the particular product $a^k b^{n-k}$ will appear: it will come from choosing a from $k$of the parentheses. There are $\binom{n}{k}$ ways of doing this. We can go from choosing no a's (or what is the same, choosing all b's) to choosing a's from all n parenntheses. This leads to the expression

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$$

as desired.

□

Example 10.15. (a) Taking $n=3$, we obtain

$$(a+b)^3=\binom{3}{0}a^3+\binom{3}{1}a^2b+\binom{3}{2}ab^2+\binom{3}{3}b^3=a^3+3a^2b+3ab^2+b^3$$

(b) Taking $n=4$, we obtain

$$(a+b)^4=\binom{4}{0}a^4+\binom{4}{1}a^3b+\binom{4}{2}a^2b^2+\binom{4}{3}ab^3+\binom{4}{4}b^4=a^4+4a^3b+6a^2b^2+4ab^3+b^4$$

(c) Applying the binomial Theorem to the expression $(1+1)^n=2^n$, we obtain

$$2^n=\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{k}+\cdots+\binom{n}{n-1}+\binom{n}{n}$$

We saw in 1.9 that the number of subsets of a set with n elements is 2^n. This gives us an interpretation for the left hand side. The terms in the right hand side $\binom{n}{k}$ is the number of ways of choosing k elements among n. So, it can be viewed as number of subsets with precisely k elements of a set with n elements. As a subsets of a set with n elements must have a number of elements k for some k with $0\leq k\leq n$, this gives a combinatorial justification of why the two expressions should agree.

In Proposition 9.3, we saw how to count the number of elements of a union of n finite sets, taking into account how they intersect. We indicated how to give a proof of the result using induction. Let us now give a combinatorial proof:

Proposition 10.16. *Assume that $A_1\dots,A_n$ are finite sets. Then $A_1\cup\cdots\cup A_n$ is finite and*

$$|A_1\cup\cdots\cup A_n|=\Sigma_{i=1}^n|A|_i-\Sigma_{i\neq j}|A_i\cap A_j|+\Sigma|A_i\cap A_j\cap A_k|+\cdots+(-1)^{n-1}|A_1\cap\cdots\cap A_n|$$

Proof. We want to make sure that we count every element x of the union exactly once. Each element of the union has to be in at least one of the sets and it can be in at most n (that is all of them). Assume that the element x is in precisely k of the sets where $1 \leq k \leq n$ and in order to make our life easier, we can assume that it is in $A_1, \ldots, A_k$ but not in $A_{k+1}, \ldots A_n$. Then, in the expression for the number of elements in the union, the element x will contribute $k = \binom{k}{1}$ times in each of $|A_1|, \ldots, |A_k|$. We will subtract the count of x for each intersection $A_1 \cap A_2, A_1 \cap A_3, \ldots, A_{k-1} \cap A_k$. There are $\binom{k}{2}$of these intersections. We will add the count of x for each triple intersection $A_1 \cap A_2 \cap A_3, \ldots, A_{k-2} \cap A_{k-1} \cap A_k$. There are $\binom{k}{3}$of these intersections. ...the count of x will contribute for the last time in the intersection $A_1 \ldots A_k$ where it appears with the sign $(-1)^{k-1}$. Therefore, the net contribution of x is

$$\binom{k}{1} - \binom{k}{2} + \binom{k}{3} - \cdots + (-1)^{k-1}\binom{k}{k}$$

Compare this expression with

$$0 = (1-1)^k = \binom{k}{0} - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} - \cdots + (-1)^k\binom{k}{k}$$

we find that

$$1\binom{k}{0} = \binom{k}{1} - \binom{k}{2} + \binom{k}{3} - \cdots + (-1)^{k-1}\binom{k}{k}$$

and as $\binom{k}{0} = 1$, it turns out we counted x exactly once, as we should. □

11. Combinations with repetition and the pigeonhole principle, Oct 20.

Definition 11.1. Given a collection A of n different types of objects and an integer k, a k **combination with repetition** of the object of of A is a set of k objects where each of the objects is of one of the n types in A and the order of the objects does not matter. The number of k combinations with repetition of n types of objects is denoted by $\left(\binom{n}{k}\right)$ ("n multichoose k").

Example 11.2. (a) Let us write all 3 combinations of the objects $\{a, b, c\}$:

$$aaa, aab, aac, abb, abc, acc, bbb, bbc, bcc, ccc$$

(b) Let us write all 4 combinations of the objects $\{a, b, c, d\}$:

$$aaaa, aaab, aaac, aaad, aabb, aabc, aabd, aacc, aacd, aadd, abbb, abbc, abbd, abcc, abcd, abdd,$$
$$accc, accd, acdd, addd, bbbb, bbbc, bbbd, bbcc, bbcd, bbdd, bccc, bccd, bcdd, bddd, cccc, cccd, ccdd, cddd, dddd$$

Proposition 11.3. *The number of k combinations with repetition of n types of objects n multichoose k is computed as*

$$\left(\binom{n}{k}\right) = \binom{n+k-1}{n-1} = \binom{n+k-1}{k}$$

Proof. We can think of having a long box that would fit $n+k-1$ of our objects. We will fill it starting from the beginnning with objects of the first kind. When we do not want any more objects of the first kind, we will fill one space with a separator and start filling with objects of the second kind and so on. We will use all of the separators. If we do not want any objects of a certain kind, we will place two separators together. There is a one to one correspondence between the spots in which we place the $k-1$ separators and the different collections. The number of ways to place the $n-1$ separators in the $n+k-1$ spots is $\binom{n+k-1}{n-1} = \binom{n+k-1}{k}$. This proves the result. □

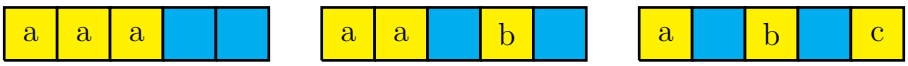


Figure 13. To obtain the combination a, a, a, place the separators in the last two spots, to obtain the combination a, a, b, place them in spots 3 and 5, to obtain a, b, c, place them in second and fourth spots

Example 11.4. (a) We want to buy a dozen donuts. There are four varieties (and at least 12 of each variety are available). In how many ways can we choose them?

This is a typical example of combinations with repetition, the answer is $\binom{12+3}{3} = \binom{15}{3} = 455$.

(b) There are four varieties of donuts available. We want to buy a dozen so that at least two are chocolate. In how many ways can we choose them?

In this case, we are not really choosing 12 donuts, two of them have been chosen before hand. We need to choose the remaining 10. As we have been asked to bring **at least** two chocolate, it is OK to choose a few that are chocolate among the 10. So, we are still choosing our 10 remaining donuts among all four varieties. We then have $\binom{10+3}{3} = \binom{13}{3} = 286$

(c) There are four varieties of donuts available. We want to buy a dozen so that at least two are chocolate and at most one is pumpkin spice. In how many ways can we choose them?

We can compute in how many ways to choose a dozen donuts so that at least two are chocolate, in how many ways to choose a dozen donuts so that at least two are chocolate and at least two are pumpkin spice and subtract the two numbers. The number we are looking for is then $\binom{10+3}{3} - \binom{8+3}{3} = \binom{13}{3} - \binom{11}{3} = 286 - 165 = 121$.

(d) In how many ways can we choose 4 natural numbers $w, x, y, z \in \mathbb{N}$ so that

$$w + x + y + z = 12,\ w \geq 2, z \leq 1?$$

This question is numerically equivalent to the previous one, so the answer is the same.

We now move to another counting technique called the pigeon hole principle. The pigeonhole principle states that if n pigeons try to nest on m holes where $n > m$, then at least two pigeons nest on the same hole. More formally:

Proposition 11.5. *A function from a set with n elements to a set nest with m elements where $n > m$ cannot be injective*

Proof. A one to one map between the two sets can be thought of as an inclusion of the domain in the codomain. We proved in Proposition 8.4 that the number of elements of a subset of a finite set is at most the number of elements of the set. Therefore, if $n > m$, the function cannot be one-to-one. □

Example 11.6. (a) There is a square room in an office building that once measured was found to be of side 8.5 feet. Let us show that , it is possible to set up to five workers but no more than this number in that room keeping the required 6 feet among any two of them. Note first that $8.5 \cong 6\sqrt{2}$ If we divide the room into 4 identical squares, each will have a side of $3\sqrt{2}$ feet. If two people are both in the same little square of the subdivision, the maximum distance they can be away from each other is

$$\sqrt{(3\sqrt{2})^2 + (3\sqrt{2})^2} = \sqrt{36} = 6.$$

Since there are five people and only four subdivision square, the pigeonhole principle says that at least one square must have two people. It follows that there must be at least two people separated by a distance of no more than 6 feet. Moreover, the distance between the two will be 6 feet if the two people are each in one corner of the subdivision. So, we can achieve the required distance by placing one worker at every corner and one at the center of the room

(b) Choosing four numbers at random in the set $\{1, 2, 3, 4, 5, 6\}$ we are guarantee to have at least one pair that adds to 7:

The pairs that add up to 7, are $\{1, 6\}, \{2, 5\}, \{3, 4\}$. There are three packs, each consiting of a pair adding to 7. If we choose four numbers, as there are only three packs, two will be in the same pack and therefore add up to seven. On the other hand, three would not be sufficient, as we could choose one from each pack, for example $1, 4, 5$.

12. Relations, equivalence relations, October 25

We will start by introducing relations in general. The mathematical concept of relation is very similar to the ordinary idea, it is a way to say that we consider the two object connected in some way. This connection can be one directional only or bi-directional for example the relation from child to parent would be of the first type, the relation among siblings would be of the second The mathematical definition is as follows

Definition 12.1. Given two sets A, B, a relation from A to B is defined to be a subset R of the cartesian product $A \times B$. We say that $a \in A$ is related to $b \in B$ and we write $a \sim b$ if and only if $(a, b) \in R$.

Example 12.2. (a) Let A be the set of all students enrolled in some class at Tufts in the Fall of 2020, B the set of all course being offered this Fall. Consider the set of pairs

$$R = \{(a, b) | a \text{ is enrolled in class } b\}$$

that is, students are related to the courses they are enrolled in. Then for any of you "your name" $\sim$ Math 65-01 holds.

(b) Let $A = \mathbb{R}^+$ the set of positive real numbers, $B = \mathbb{Z}$ the integers. Consider the set of pairs

$$R = \{(a, b) \in \mathbb{R}^+ \times \mathbb{Z} | b \leq a \leq b + 1\}$$

that is, every real number is related to the integers that are at most one unit apart from it.Then $1.3 \sim 1, 1.3 \sim 2$ but $1.3 \not\sim 5$.

(c) Let A, B be two arbitrary sets, $f : A \to B$ a function. The relation

$$R = \{(a, b) \in A \times B | b = f(a)\}$$

is called the graph of the function. It satisfies the condition that every $a \in A$ appears exactly once as the first term of a pair in R.

For instance if $A = \{a, b, c\}, B = \{1, 2, 3\}, R_1 = \{(a, 1), (b, 1), (c, 3)\}$ is the graph of a function. But if $A = \{a, b, c\}, B = \{1, 2, 3\}, R_2 = \{(a, 1), (a, 2), (b, 3), (c, 3)\}$ is not the graph of a function as a appears twice as the first term of a pair. Similarly, if $A = \{a, b, c\}, B = \{1, 2, 3\}, R_2 = \{(a, 1), (b, 3)\}$ is not the graph of a function as c does not appear as the first term of a pair(see Figure 6).

In the case when you have a function from $\mathbb{R} \to \mathbb{R}$ this definition of graph is the graph in the plane $\mathbb{R}^2$ that you are familiar with. The condition that for every $a \in A$, a appears in one and only one pair $(a, b) \in R$ is a translation of the vertical line test

We now focus on relations of objects of a single set (that is $A = B$). These relations may or may not satisfy the following properties

Definition 12.3. Given a set A with a relation $\sim$, we say that

(a) The relation is **reflexive** if every element is related to itself $\forall a \in A,\ a \sim a$.
(b) The relation is **symmetric** if $\forall a_1, a_2 \in A, a_1 \sim a_2 \Rightarrow a_2 \sim a_1$.
(c) The relation is **antisymmetric** if $\forall a_1, a_2 \in A, a_1 \sim a_2$ and $a_2 \sim a_1 \Rightarrow a_1 = a_2$.
(d) The relation is **transitive** if $\forall a_1, a_2, a_3 \in A, a_1 \sim a_2$ and $a_2 \sim a_3 \Rightarrow a_1 \sim a_3$

Example 12.4. (a) if $A = \{a, b, c\}, R_1 = \{(a, b), (b, c), (c, a)\}$, then R_1 is neither reflexive (it does not contain (a, a)), nor symmetric (it contains (a, b) but not (b, a)). But the relation is antisymmetric as it does not contain any pairs (x, y) and (y, x) with $x \neq y$.

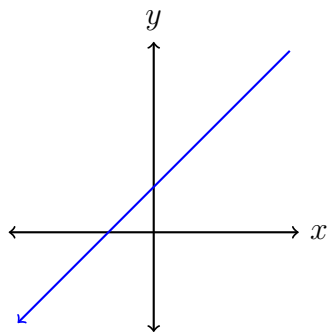


FIGURE 14. The graph of the function $f(x) = x + 1$. consists of all pairs of points in the plane with coordinates $(x, x + 1), x \in \mathbb{R}$.

It is also transitive as the only pairs $(x, y), (y, z)$ are $(a, b), (b, c)$ and the element (a, c) is also in the relation.

(b) if $A = \{a, b, c\}, R_2 = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$, then R_2 is reflexive, symmetric and transitive.

(c) if $A = \{a, b, c\}, R_3 = \{(a, a), (b, b), (c, c)\}$, then R_1 is reflexive, symmetric, antisymmetric and transitive.

Definition 12.5 (Equivalence Relation)**.** Given a set A with a relation $\sim$, we say that $\sim$ is an equivalence relation if it satisfies the following 3 properties

- It is reflexive, that is, every element is related to itself $\forall a \in A,\ s \sim s$.
- It is symmetric $\forall a_1, a_2 \in A, a_1 \sim a_2 \Rightarrow a_2 \sim a_1$
- It is transitive $\forall a_1, a_2, a_3 \in A, a_1 \sim a_2$ and $a_2 \sim a_3 \Rightarrow a_1 \sim a_3$

Example 12.6. (a) In the set of all students at Tufts, we will say that student x is related to student y if both students are enrolled in at least one section of the same course. This relation is reflexive and symmetric but not transitive as for instance students x, y may both be enrolled in Math 61, students y, z may both be enrolled in Comp 40 but perhaps students x, z are not enrolled in any common course.

(b) In the set of all students at Tufts, we will say that student x is related to student y if both students are enrolled in the same courses this semester. This relation is reflexive, symmetric and transitive.

(c) Consider the following relation R on the set $A = \{a, b, c\}$. $R = \{(a, a), (a, b), (b, b), (b, a), (c, c)\}$.

- The relation is reflexive as it contains $(a, a), (b, b), (c, c)$.
- The relation is symmetric: the only pairs $(x, y), x \neq y$ in the relation are $(a, b), (b, a)$ satisfying the condition that $x \sim y$ implies $y \sim x$ (or equivalently that with (x, y), the relationn also contains (y, x)).
- The relation is transitive: the only pairs $(x, y), x \neq y$ in the relation are $(a, b), (b, a)$, that is $a \sim b$ and $b \sim a$ which implies if the relation is transitive $a \sim a$. Also $b \sim a$ and $a \sim b$ implies if the relation is transitive $b \sim b$. As the relation contains both (a, a) and (b, b),it is transitive

As the relation is reflexive, symmetric and transitive, it is an equivalence relation.

(d) Consider the set $S = \mathbb{Z}$ of all integers. Choose a **fixed** integer n. Define the relation

$$z_1, z_2 \in \mathbb{Z}, \text{ then } z_1 \sim z_2 \iff \exists k \in \mathbb{Z}, z_1 - z_2 = nk.$$

We check that it is an equivalence relation by checking that it satisfies the three properties of the definiton

- It is reflexive, $\forall z \in \mathbb{Z}, z - z = 0 = n0$. As 0 is an integer, from the definition of the relation $\forall z \in \mathbb{Z},\ z \sim z$.
- It is symmetric $\forall z_1, z_2 \in \mathbb{Z}, z_1 \sim z_2$ means that $\exists k \in \mathbb{Z}, z_1 - z_2 = nk$ Then

$$\exists k \in \mathbb{Z}, z_2 - z_1 = -(z_1 - z_2) = -nk = n(-k).$$

  If $k \in \mathbb{Z}$, then also $-k \in \mathbb{Z}$. So, by the definition of the relation $z_2 \sim z_1$ and therefore the relation is symmetric.
- It is transitive: Assume $z_1, z_2, z_3 \in \mathbb{Z}, z_1 \sim z_2$ and $z_2 \sim z_3$ By definition of the relation, there exist integers k_1, k_2 such that $z_1 - z_2 = nk_1, z_2 - z_3 - nk_2$. Adding these two equations, one obtains

$$z_1 - z_3 = (z_1 - z_2) + (z_2 - z_3) = nk_1 + nk_2 = n(k_1 + k_2)$$

  As $k_1 + k_2 \in \mathbb{Z}$, the definition of our relation implies that $z_1 \sim z_3$ and therefore the relation is transitive.

(e) Let $A = \mathbb{Z} \times (\mathbb{Z} - \{0\})$ be the set of pairs of integers with the second one not being zero. Define a relation $\sim$ on A as follow: $(a, b) \sim (c, d)$ if and only if $ad = bc$. Let us now be careful in checking the three properties of an equivalence relation for $\sim$. As A is a set of pairs, the relation relates two pairs.

- The relation is reflexive: assume $(a, b) \in A$. Then $ab = ba$ by the commutative property of the product of integers. Hence, by definition of the relation, $(a, b) \sim (a, b)$. Therefore, $\sim$ is reflexive.
- The relation is symmetric: assume $(a, b), (c, d) \in A$ and $(a, b) \sim (c, d)$. By definition of $\sim$, this means $ad = bc$. Hence, $cb = da$. Therefore, by definition of $\sim$, $(c, d) \sim (a, b)$.
- The relation is transitive: assume $(a, b), (c, d), (e, f) \in A$ and $(a, b) \sim (c, d),\ (c, d) \sim (e, f)$. By definition of $\sim$, this means $ad = bc,\ cf = de$. Multiplying the first equation with f and the second with b, we obtain $adf = bcf,\ bcf = bde$. Therefore, $adf = bde$. This is equivalent to $d(af - be) = 0$. As by assumption, $d \neq 0$, $af - be = 0$ or $af = be$. By definition of $\sim$, this means that $(a, b) \sim (e, f)$. Hence the transitive property holds.

As the relation is reflexive, symmetric and transitive, it is an equivalence relation.

Definition 12.7 (Equivalence classes)**.** Given an equivalence relation on a set A we define subsets of A as follows: the **equivalence class** of $a \in A$ denoted by $[a]$ consists of the set of all elements in A that are related to a

$$[a] = \{x \in A \text{ such that } x \sim a\}$$

The equivalence class of a is also called the **coset** of a by the equivalence relation.

Example 12.8. We will look at the equivalence classes for the examples in 12.6

(a) In the example above, we showed that (a) was not an equivalence relation. Therefore, it does not make sense to talk about equivalence classes.

(b) In example (b) there are many different equivalence classes, one for any actual class choice at Tufts this semester. Many of the cosets have only one element, some have many, corresponding to the most popular course choices or the more restrictive majors.

(c) For the relation R on the set $A = \{a, b, c\}$. $R = \{(a, a), (a, b), (b, b), (b, a), (c, c)\}$. the equivalence classes are

$$[a] = [b] = \{a, b\}, [c] = \{c\}$$

(d) In the relation $\sim$ in $A = \mathbb{Z} \times (\mathbb{Z} - \{0\})$ defined a relation $\sim$ by $(a, b) \sim (c, d)$ if and only if $ad = bc$, the equivalence classes will become familiar if instead of writing (a, b) you write $\frac{a}{b}$. The condition that $b \neq 0$ means that the fraction makes sense and the equivalence relation is precisely the equality of fractions. The set of equivalence classes is nothing else that the set of rational numbers.

We will see in the next section that the set of equivalence classes by an equivalence relation on a given set allow to classify the elements of the set by dividing them into subsets that are disjoint and cover the whole set. Moreover, the set of equivalence classes is itself a new set, sometimes more interesting that the set we started with. For example the rational numbers are far more useful than the set of fractions that gave rise to them.

13. Equivalence classes, October 27

Given a set A and an equivalence relation $\sim$ in Definition 12.7 we defined the equivalence class or coset of $a \in A$ as the set of all elements in A that are related to a

$$[a] = \{x \in A \text{ such that } x \sim a\}$$

We start with some important properties of equivalence classes as follows:

Proposition 13.1. *Let A be a set with an equivalence relation $\sim$. Then the following hold:*
(a) For all $a \in A, a \in [a]$.
(b) $a \in [b] \iff a \sim b \iff b \in [a]$.
(c) If $a \in [b]$ then $[a] = [b]$.
(d) Two equivalence classes are either disjoint or the same

Proof. We will prove each of the statements in order:

(1) From the reflexive property of an equivalence relation, $\forall a \in A,\ a \sim a$. Therefore, from the definition of equivalence class, $a \in [a]$.
(2) Assume $a \in [b]$. From the definition of equivalence class $[b]$, this means that $a \sim b$. From the symmetric property of an equivalence relation, this implies that $b \sim a$. From the definition of equivalence class $[a]$, this implies that $b \in [a]$. We can then reverse the roles of a and b to prove the equivalence in the other direction.
(3) We first show that if $a \in [b]$ then $[a] \subset [b]$: Let $x \in [a]$. By definition of the equivalence class $[a]$, this means that $x \sim a$. As we are assuming that $a \in [b]$, we have $a \sim b$. Therefore, by the transitive property, $x \sim b$. Then by definition of the equivalence class $[b]$, $x \in [b]$. As x was an arbitrary element of $[a]$, this shows that $[a] \subset [b]$. Using the prior statement, we can reverse the roles of a, b and therefore get the opposite inclusion. We then deduce that $[a] = [b]$.
(4) Assume two equivalence classes $[a], [b]$ are not disjoint. Then we can find $x \in S$ such that $x \in [a] \cap [b]$. The previous property implies then that $[x] = [a]$ and $[x] = [b]$. Therefore $[a] = [b]$.

□

Example 13.2. We saw in Example 12.6 (e) that in the set $S = \mathbb{Z}$ of all integers, after choosing a fixed integer n, the relation

$$z_1, z_2 \in \mathbb{Z}, \text{ then } z_1 \sim z_2 \iff \exists k \in \mathbb{Z}, z_1 - z_2 = nk.$$

is an equivalence relation. There are n equivalence classes $[0], [1], \ldots [n-1]$. We can check that the elements $0, 1, \ldots, n-1 \in \mathbb{Z}$ are not related to each other as the difference of any two of them is less than n and therefore not divisible by n unless it is 0. Now, given any integer z, using long division by n, we can find a quotient $q \in \mathbb{Z}$ and a remainder $r \in \mathbb{Z}$ such that $z = qn + r, 0 \leq r \leq n-1$. Therefore, $z - r = qn$. From the definition of the equivalence relation $z \in [r]$ and from the definition of remainder, $r \in \{0, 1, \ldots, n-1\}$. For example, the equivalence class of 0 is the set of all multiples of n:

$$[0] = \{x \in \mathbb{Z} \text{ such that } \exists k \in \mathbb{Z}\ x - 0 = nk\} = n\mathbb{Z}$$

We will use the notation $[\ ]_n$ when necessary to indicate equivalence classes and avoid confusions about the n we are talking about.

This set of all equivalence classes is denoted by $\mathbb{Z}_n$.

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \dots [n-1]_n\}$$

The first and last property in Proposition 13.1 together tell us that every element in A is in one and only one equivalence class. So A is the disjoint union of all the equivalence classes of elements in A. This gives us a way of classifying the elements in A according to the equivalence class to which they belong. It also gives rise to the construction of new sets, the set of equivalence classes which often has a live of its own. For example, as we have seen in Examples 12.6, 12.8 (d), the rational numbers $\mathbb{Q}$ is the set of equivalence classes of an equivalence relation defined on the set $A = \mathbb{Z} \times (\mathbb{Z} - \{0\})$, otherwise known as the set of fractions.

Working with equivalence classes is often important. It is also tricky if the only way we have of getting hold of an equivalence class is by taking a representative of that equivalence class. For example, let x, y be rational numbers $x, y \in \mathbb{Q}$. We want to define their sum and product using what we already know from addition and product of integers. This is normally done as follows: as x, y are rational, we can find integers $a, b, c, d \in \mathbb{Z}, b \neq 0, d \neq 0$ such that x can be represented by $\frac{a}{b}$ and y can be represented by $\frac{c}{d}$. Then we say that $x + y$ is the rational number represented by $\frac{ad+bc}{bd}$ and xy is the rational number represented by $\frac{ac}{bd}$. We need to make sure that this makes sense. For example, both $\frac{1}{2}, \frac{2}{4}$ represent the same rational number that we will call x. Both $\frac{15}{25}, \frac{3}{5}$ represent the same rational number that we will call y. Then we want $x + y$ to be represented by both

$$\frac{1 \times 25 + 2 \times 15}{2 \times 25} = \frac{55}{50}, \ \frac{2 \times 5 + 4 \times 3}{4 \times 5} = \frac{22}{20}$$

which is OK as both fractions represent the same rational number.

Similarly, we want xy to be represented by both

$$\frac{1 \times 15}{2 \times 25} = \frac{15}{50}, \ \frac{2 \times 3}{4 \times 5} = \frac{6}{20}$$

which is again OK as both fractions represent the same rational number.

In general, if we want the sums and products of rational numbers to be well defined in terms of the operations with the corresponding fractions, we need the following result

Proposition 13.3. *Let $a_1, a_2, c_1, c_2 \in \mathbb{Z}, \ b_1, b_2, d_1, d_2 \in \mathbb{Z} - \{0\}$ be such that the fractions $\frac{a_1}{b_1}, \frac{a_2}{b_2}$ are equivalent fractions, that is $a_1 b_2 = a_2 b_1$ and $\frac{c_1}{d_1}, \frac{c_2}{d_2}$ are equivalent fractions, that is $c_1 d_2 = c_2 d_1$ Then*

$$\frac{a_1 d_1 + c_1 b_1}{b_1 d_1}, \ \frac{a_2 d_2 + c_2 b_2}{b_2 d_2}$$

are equivalent fractions, and so are

$$\frac{a_1 c_1}{b_1 d_1}, \ \frac{a_2 c_2}{b_2 d_2}$$

Proof. We look at addition first. We start with the two equations

$$a_1 b_2 = a_2 b_1, \ c_1 d_2 = c_2 d_1$$

We multiply the first equation by $d_1 d_2$ and the second one with $b_1 b_2$ and we obtain

$$a_1 b_2 d_1 d_2 = a_2 b_1 d_1 d_2, \ c_1 d_2 b_1 b_2 = c_2 d_1 b_1 b_2$$

Adding the left hand sides and right hand sides of the two equations and using the distributive property, we obtain

$$b_2d_2(a_1d_1 + c_1b_1) = a_1b_2d_1d_2 + c_1d_2b_1b_2 = a_2b_1d_1d_2 + c_2d_1b_1b_2 = b_1d_1(a_2d_2 + c_2b_2)$$

which says that the two fractions $\frac{a_1d_1+c_1b_1}{b_1d_1}$, $\frac{a_2d_2+c_2b_2}{b_2d_2}$ are equivalent. Hence, addition of rational numbers is well defined.

Similarly, starting again from $a_1b_2 = a_2b_1,\ c_1d_2 = c_2d_1$ and multiplying the left and right hand sides of these equations, we obtain

$$a_1b_2c_1d_2 = a_2b_1c_2d_1$$

which says that the fractions $\frac{a_1c_1}{b_1d_1}$, $\frac{a_2c_2}{b_2d_2}$ are equivalent. Hence, product of rational numbers is well defined. □

Example 13.4. We define addition on $\mathbb{Z}_n$ as follows

$$[a]_n + [b]_n = [a + b]_n$$

We need to check that this makes sense: An equivalence class can be represented by many different integers. We need to verify that the elements we pick to represent the equivalence classes do not change the definition of the operation. Let us assume that $[a_1]_n = [a_2]_n,\ [b_1]_n = [b_2]_n$. Recall that two equivalence classes are the same if the elements are related. From our definition of the equivalence relation

$$\exists k \in \mathbb{Z}, a_1 - a_2 = nk, \exists l \in \mathbb{Z}, b_1 - b_2 = nl$$

Adding these two equations we obtain

$$(a_1 + b_1) - (a_2 + b_2) = n(k + l).$$

As $k + l$ is the sum of two integers, it is again an integer. Then, from the definition of the equivalence relation, this tells us that $a_1 + b_1 \sim a_2 + b_2$ or equivalently $[a_1 + b_1]_n = [a_2 + b_2]_n$. Therefore, the definition $[a]_n+[b]_n = [a+b]_n$ defines the sum of cosets in an unambiguous way, it does not matter if we change the integer so long as we stay inside each of the equivalence classes, we still get the same equivalence class for the sum.

We now define product on $\mathbb{Z}_n$ as follows

$$[a]_n[b]_n = [ab]_n$$

We check that this is well defined. Let us assume that $[a_1]_n = [a_2]_n,\ [b_1]_n = [b_2]_n$. Then, $\exists k \in \mathbb{Z}, a_1 - a_2 = nk, \exists l \in \mathbb{Z}, b_1 - b_2 = nl$. We can rewrite these equations as

$$\exists k \in \mathbb{Z}, a_1 = a_2 + nk, \exists l \in \mathbb{Z}, b_1 = b_2 + nl$$

Multiplying these two equations we obtain

$$a_1b_1 = a_2b_2 + na_2l + nkb_1 + n^2kl = a_2b_2 + n(a_2l + b_2k + nkl)$$

As a_1, b_1, k, l, n are integers,$a_2l + b_2k + nkl$ is also an integer. Then, from the definition of the equivalence relation, this tells us that $a_1b_1 \sim a_2b_2$ or equivalently $[a_1b_1]_n = [a_2b_2]_n$. Therefore, setting $[a]_n[b]_n = [ab]_n$ defines the product of cosets in an unambiguous way,

The arithmetic properties of addition and product in $\mathbb{Z}_n$ is called modular arithmetic. Modular arithmetic is widely used in cryptography and error correction. Instead of checking that two numbers are the same, it is easier to check that their cosets are the same in $\mathbb{Z}_n$ for some n. For a general interest article, you can read

https://www.irishtimes.com/news/science/modular-arithmetic-you-may-not-know-it-but-you
3268649

There are also more sophisticated generalizations that those of you in a computer science track may be more interested in. For example, you can read

https://en.wikipedia.org/wiki/Modulo_operation

14. Partial Orders November 1

We saw that an important type of relations are equivalence relations, as they allow to classify objects. In this section we focus on a different type, namely partial orders

Definition 14.1 (Partial Order)**.** Given a set A with a relation $\preceq$, we say that $\preceq$ is a **partial order** in A if it satisfies the following 3 properties

- It is reflexive, that is, every element is related to itself $\forall a \in A,\ a \preceq a$.
- It is antisymmetric $\forall a_1, a_2 \in A, a_1 \preceq a_2$ and $a_2 \preceq a_1 \Rightarrow a_1 = a_2$
- It is transitive $\forall a_1, a_2, a_3 \in A, a_1 \preceq a_2$ and $a_2 \preceq a_3 \Rightarrow a_1 \preceq a_3$

The pair of a set and a partial order relation $(A, \preceq)$ is called a **poset**.

Example 14.2. (a) The ordering you are most familiar with is the one in the sets of numbers $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

The complex numbers on the other hand do not have a natural order. We have a way to measure how big a complex number is by its norm (or distance to the origin in the plane representation) $|a + bi| = \sqrt{a^2 + b^2}$. If we try to define $a + bi \preceq c + di$ when $|a + bi| \leq |c + di|$ we do not obtain a partial order as the relation is not antisymmetric. For example, $|1| = |i|$ but $1 \neq i$.

(b) Consider the set of strictly positive natural numbers $\mathbb{N} - \{0\}$. For $a, b \in \mathbb{N} - \{0\}$, we define $a \preceq b$ if and only if a divides b. Then, $(\mathbb{N} - \{0\}, \preceq)$ is a coset:
- The relation is reflexive: for all $a \in \mathbb{N} - \{0\}$, $a = 1 \times a, 1 \in \mathbb{N}$. So a divides itself. By definition of the relation, this means that $\forall a \in A,\ a \preceq a$.
- The relation is antisymmetric $\forall a_1, a_2 \in \mathbb{N} - \{0\}, a_1 \preceq a_2$ and $a_2 \preceq a_1$ means that $\exists k, l \in \mathbb{N}$ such that $a_2 = ka_1, a_1 = la_2$. Then, $a_1 = la_2 = (lk)a_1$. So, $a_1 = lka_1, a_1(1 - lk) = 0$. As $a_1 \neq 0, 1 - lk = 0$ so $lk = 1$. As $l, k \in \mathbb{N}$ this means that $k = l = 1$ and therefore $a_1 = a_2$, showing that the relation is antisymmetric.
- The relation is transitive $\forall a_1, a_2, a_3 \in \mathbb{N} - \{0\}, a_1 \preceq a_2$ and $a_2 \preceq a_3$ means that $\exists k, l \in \mathbb{N}$ such that $a_2 = ka_1, a_3 = la_2$. Then, $a_3 = la_2 = (lk)a_1$. As $l, k \in \mathbb{N},\ lk \in \mathbb{N}$. Then, by definition of the relation, $a_1 \preceq a_3$ showing that the relation is trannsitive. A relation that is reflexive, symmetric and transitive is a partial order

(c) Let A be any set, $\mathcal{P}(A)$ the set of all subsets of A. Consider the inclusion relation

$$A_1, A_2 \in \mathcal{P}(A), \quad A_1 \preceq A_2 \ \Leftrightarrow A_1 \subseteq A_2$$

Then, $(\mathcal{P}(A), \preceq)$ is a poset.
- As for every subset X, $X \subseteq X$, the relation is reflexive.
- By definition of equality of sets , $X \subseteq Y$ and $Y \subseteq X$ implies $X = Y$. Hence the relation is antisymmetric.
- If $X \subseteq Y$ and $Y \subseteq Z$ then $X \subseteq Z$. So, inclusion is transitive.

Therefore, $(\mathcal{P}(A), \preceq)$ is a poset.

The ordering of numbers in the real line is special in the sense that given two real numbers $a, b \in \mathbb{R}$, either $a \leq b$ or $b \leq a$. This is not true for the second example of divisibility of natural numbers: 2 does not divide 3 and 3 does not divide 2, so 2 and 3 are not comparable by the order defined by divisibility. We have a name for when any two elements are comparable:

Definition 14.3. Given a poset $(A, \preceq)$, we say that A is **totally ordered** if $a, b \in A$, you always have either $a \preceq b$ or $b \preceq a$.

Given a partially ordered set $(A, \preceq)$, a subset $C \subseteq A$ is called a **chain** if the restriction of the ordering to C is a total ordering That means that $\forall c_1, c_2 \in C$, either $c_1 \preceq c_2$ or $c_2 \preceq c_1$.

Given a partially ordered set $(A, \preceq)$, a subset $D \subseteq A$ is called an **antichain** if in the restriction of the ordering to D every element is only related to itself. That means that $\forall d_1, d_2 \in C$, $d_1 \preceq d_2 \ \Rightarrow \ d_1 = d_2$.

Example 14.4. (a) Consider the set of strictly positive natural numbers $\mathbb{N} - \{0\}$ with the relation defined by $a \preceq b$ if and only if a divides b. Then the set $\{2^n | n \in \mathbb{N}\}$ is a chain as $2^n = 2^{n-m}2^m$ if $n \geq m$. So

$$2^m \preceq 2^n, m \leq n, \quad 2^n \preceq 2^m, n \leq m$$

(b) Consider the set of strictly positive natural numbers $\mathbb{N} - \{0\}$ with the relation defined by $a \preceq b$ if and only if a divides b. Then the set of prime numbers is an antichain as a prime number is only divisible by 1 and the number itself and 1 is not in the set.

Partial orders can be graphically displayed using **Hasse diagrams** that shows a segment among related elements and places the "largest" object higher that the "smaller" object For example, the Hasse diagram for the order of divisibility on the set $\{2, 3, 4, 5, 6, 12\}$ would look like

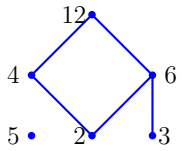


FIGURE 15. The Hasse diagram for divisibility for the set $\{2, 3, 4, 5, 6, 12\}$

We define next the concepts of being the smallest or largest element in a set as well as not being smaller than anything or not being larger than anything

Definition 14.5. (a) An element $x \in X$ is maximal if there is nothing strictly above it, that is if any $y \in X$ satisfies $x \preceq y$, then $x = y$.
(b) An element $x \in X$ is a maximum if it is above everything else, that is $\forall y \in X, \ y \preceq x$.
(c) An element $x \in X$ is minimal if there is nothing strictly below it, that is if for any $y \in X$ that satisfies $y \preceq x$, then $x = y$.
(d) An element $x \in X$ is a minimum if it is below everything else, that is $\forall y \in X, \ x \preceq y$.

Example 14.6. (a) In the ordering by divisibility in the set $\{2, 3, 4, 5, 6, 12\}$, 2, 3, 5 are minimal, 5 and 12 are maximal, there is neither a maximum nor a minimum
(b) In the usual ordering of the natural numbers, 0 is a minimum, there is no maximum

Proposition 14.7. *Consider a poset $(A, \preceq)$*
(a) If $a \in A$ is a minimum, then a is minimal.
(b) If $b \in A$ is a maximum, then b is maximal.
(c) The minimum of A, if it exists is unique.
(d) The maximum of A, if it exists is unique.

Proof. (a) Assume that $a \in A$ is a minimum. By definition of minimum, for all $x \in A$, $a \preceq x$. Assume there is some $y \in A$ with $y \preceq a$. Then we have both $y \preceq a, a \preceq x$. By the antisymmetric property, then $a = y$. Then, from the definition of minimal, a is minimal.

(b) Assume that $b \in A$ is a maximum. By definition of maximum, for all $x \in A$, $x \preceq b$. Assume there is some $y \in A$ with $b \preceq y$. Then we have both $y \preceq b, b \preceq x$. By the antisymmetric property, then $a = y$. Then, from the definition of maximal, b is maximal.

(c) Assume that a, a' are both minimums, we need to show they are equal. As a is a minimum, for all $x \in A$, $a \preceq x$. In particular $a \preceq a'$.

As a' is a minimum, for all $x \in A$, $a' \preceq x$. In particular $a' \preceq a$. Then, from the antisymmetric property, $a' = a$. So, the minimum of A, if it exists is unique.

(d) Assume that b, b' are both maximums, we need to show they are equal. As b is a maximum, for all $x \in A$, $x \preceq b$. In particular $b' \preceq b$.

As b' is a maximum, for all $x \in A$, $x \preceq b'$. In particular $b \preceq b'$. Then, from the antisymmetric property, $b = b'$. So, the maximum of A, if it exists is unique.

□

We see in the proofs of the Proposition above that the proofs of the results for maximum and minimum are very similar, just with the inequalities reversed. and the same can be said for the proofs for maximal and minimal. This is not by chance, reversing the inequalities in a partial order, we get another partial order. In such a reversal, the roles of maximum and minimum get interchannged and the roles of maximal and minimal get interchanged.

Proposition 14.8. *Consider a poset $(A, \preceq)$. For $a, b \in A$, define $a \preceq' b \Leftrightarrow b \preceq a$*

(a) The pair $(A, \preceq')$ is a poset.
(b) If $a \in A$ then a is a minimum for $\preceq$, if and only if a is maximum for $\preceq'$.
(c) If $b \in A$, then b is a maximum for $\preceq$, if and only if b is minimum for $\preceq'$.
(d) If $a \in A$ then a is minimal for $\preceq$, if and only if a is maximal for $\preceq'$.
(e) If $b \in A$, then b is maximal for $\preceq$, if and only if b is minimal for $\preceq'$.

Proof. (a) We check the three conditions for a partial order for $\preceq'$.

- It is reflexive,: as $\preceq$ is reflexive, $\forall a \in A,\ a \preceq a$. But interchanging the two sides in this expression nothing changes $a \preceq' a$. Therefore, $\preceq'$ is reflexive.
- It is antisymmetric: assume that $a_1 \preceq' a_2$ and $a_2 \preceq' a_1$. By definition of $\preceq'$, this means that $a_2 \preceq a_1$ and $a_1 \preceq a_2$. As $\preceq$ is antisymmetric, this implies that $a_2 = a_1$. Therefore, $\preceq'$ is antisymmetric.
- It is transitive: Assume that $a_1, a_2, a_3 \in A, a_1 \preceq' a_2$ and $a_2 \preceq' a_3$. By definition of $\preceq'$, this means that $a_2 \preceq a_1$ and $a_3 \preceq a_2$. As $\preceq$ is transitive, this implies that $a_3 \preceq a_1$. Then, by definition of $\preceq'$, $a_1 \preceq' a_3$, so $\preceq'$ is transitive as claimed.

(b) Given $a \in A$, a is a minimum for $\preceq$, if and only if for all $x \in A$, $a \preceq x$. By definition of $\preceq'$, this means that for all $x \in A$, $x \preceq' a$. This is the definition of a being a maximum for $\preceq'$.

(c) As the process of going from $\preceq$ to $\preceq'$ is its own inverse, (c) follows from part (b).

(d) Assume that $a \in A$ is minimal for $\preceq$. By definition of minimal, this is equivalent to saying that for any $x \in A$ satisfying $x \preceq a$ satisfies $x = a$. By definition of $\preceq'$, this

means that for all $x \in A$ satisfying $a \preceq' x$, we get $x = a$. This is the definition of a being maximal for $\preceq'$.

(e) As the process of going from $\preceq$ to $\preceq'$ is its own inverse, (e) follows from part (d).

□

Example 14.9. (a) We can order numbers by $\geq$ meaning that we define $a \preceq b$ if annd only if $a \geq b$. This gives posets to $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$. In $\mathbb{N}$ 1 would be maximal and a maximum by this relation, nno minimum exists. In the other sets of numbers, there are no maximal or minimal elements for the whole set.

(b) In the set of strictly positive natural numbers $\mathbb{N} - \{0\}$, for $a, b \in \mathbb{N} - \{0\}$, we can define $a \preceq b$ if and only if a is divisible by b. The Hasse diagram for the subset $\{2, 3, 4, 5, 6, 12\}$ would be obtained by turning upside down the Hasse diagram in Figure 15

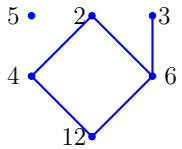


FIGURE 16. The Hasse diagram for "being divisible by" for the set $\{2, 3, 4, 5, 6, 12\}$

In this subset, $2, 3, 5$ are maximal, $5, 12$ minimal.

(c) Let A be any set, $\mathcal{P}(A)$ the set of all subsets of A. The "being contained " relation

$$A_1, A_2 \in \mathcal{P}(A), \quad A_1 \preceq A_2 \Leftrightarrow A_1 \supseteq A_2$$

Then, $(\mathcal{P}(A), \preceq)$ is a poset. The empty set is a maximum and the set A a minimum in this relation.

15. Probability, November 3

From an intuitive point of view, probability is a way to measure how likely to occur is a random event. For example, a standard die is a cube with dots on each face so that each of the possibilities of one to six dots appears in one face. If the die is completely symmetric, when tossing it, each face has the same chances to come up on top. Therefore, probability of getting a 3 showing up is $\frac{1}{6}$.

Assume now that you toss two dice and add the number of dots that appear among the two. We want to compute the probability that the sum is 5. In this case, there are 36 possible ways in which the pair of dice can come up, each equally likely. The sum adds up to 5 for the options $1+4, 2+3, 3+2, 4+1$, that is, in 4 of the 36 options. Then, the probability of getting a sum of 5 is $\frac{4}{36} = \frac{1}{9}$.

Mathematicians model random events with a sample space or probability space. We will consider only finite sample spaces:

Definition 15.1. A **sample space** is a pair (S, P) where S is a set and $P : S \to \mathbb{R}$ is a function satisfying

- For every $s \in S, 0 \leq P(s) \leq 1$.
- $\sum_{s \in S} P(s) = 1$

The idea is that the set S represents the different possible things that can occur and the number measures how likely is each of them to happen. The condition that the sum is one reflects that one things will certainly happen, we do not know which one.

Example 15.2. (a) The toss of a die can be modeled with a sample space

$$S = \{1, 2, 3, 4, 5, 6\},\ P(n) = \frac{1}{6}, n = 1, \ldots, 6$$

(b) The toss of two dice can be modeled with the sample space

$$S = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\},$$

$$P(2) = \frac{1}{36} = P(12),\ P(3) = \frac{2}{36} = \frac{1}{18} = P(11),\ P(4) = \frac{3}{36} = \frac{1}{12} = P(10),\ P(5) = \frac{4}{36} = \frac{1}{9} = P(9),$$

$$P(6) = \frac{5}{36} = P(8),\ P(7) = \frac{6}{36} = \frac{1}{6}$$

Definition 15.3. An **event** is a subset of the sample space $E \subseteq S$. The probability of an event is the sum of the probabilities of its elements $P(E) = \sum_{e \in E} P(e)$.

The second condition in the definition of probability implies that the probability of the event S is 1, that is one of the possible options must occur with complete certainty.

Example 15.4. (a) When tossing a die, the probability that it comes up an even number is

$$P(\{2, 4, 6\}) = P(2) + P(4) + P(6) = \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = \frac{1}{2}$$

(b) When tossing two dice, the probability that the sum is an even number is

$$P(\{2, 4, 6, 8, 10, 12\}) = P(2)+P(4)+P(6)+P(8)+P(10)+P(12) = \frac{1}{36}+\frac{3}{36}+\frac{5}{36}+\frac{5}{36}+\frac{3}{36}+\frac{1}{36} = \frac{1}{2}$$

Some properties that follow from the definition

Proposition 15.5. *(a) The probability of the complement of an event is 1 minus the probability of the event* $P(\bar{A}) = 1 - P(A)$.
(b) The empty set has probability zero $P(\emptyset) = 0$.
(c) The probability of the union is the sum of the probabilities of the two events minus the probability of the intersection $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

Proof. (a) Given $A \subseteq S$, by definition of probability of an event, $P(A) = \sum_{a \in A} P(a)$. Similarly, $P(\bar{A}) = \sum_{a \in \bar{A}} P(a)$. As every element in S is in A or in $\bar{A}$ but not in both and the sum of the probabilities of the elements in S add to one,

$$P(A) + P(\bar{A}) = \sum_{a \in \bar{A}} P(a) + \sum_{a \in \bar{A}} P(a) = \sum_{a \in S} P(a) = 1.$$

(b) The probability of the empty set is computed by taking a sum over an empty set of indices, therefore, it is 0.
(c) The probability of the union is the sum of the probabilities of the elements in either set, each taken once. The sum of the probabilities of A, B is the sum of the probabilities of the elements in either set, with the elements in the intersection appearing twice, once coming from the probability of A and the other from B. Hence,

$$P(A \cup B) + P(A \cap B) = P(A) + P(B).$$

□

Example 15.6. (a) When tossing two dice the probability that the sum is at least four is the complement of the probability that it is 2 or 3, that is

$$P(\geq 4) = 1 - P(\{2, 3\}) = 1 - (\frac{1}{36} + \frac{3}{36}) = 1 - \frac{4}{36} = \frac{8}{9}.$$

(b) Lunch boxes are being packed with a fruit and a sandwich. The fruit is an apple an orange or a pear and the sandwiches are tuna, ham or cheese. Your favorites are pear and tuna. If all options of fruit are equally likely and same for all options of sandwich filling, what are the chances that you get at least one of your top choices?

As all options of fruit are equally likely, the probability of getting a pear is $\frac{1}{3}$. Similarly, the probability of getting tuna is $\frac{1}{3}$. In this case, pairing each fruit with each filling there are 9 options, all equally likely. So the probability of getting tuna AND a pear is $\frac{1}{9}$. Then,

$$P(\text{ pear or tuna}) = P(\text{ pear}) + P(\text{ tuna}) - P(\text{ pear AND tuna}) = \frac{1}{3} + \frac{1}{3} - \frac{1}{9} = \frac{5}{9}$$

that is you have a little over a half chance of getting at least one of your favorites but only $\frac{1}{9}$ of getting both.

When trying to compute the probability of a certain condition in a subset of the set of events, the number to consider may be different that the probability in the whole set. For example, the probability of serious complications for a 12 years old girl sick with Covid19 is much lower than the probability for a 90 years old man. To measure this differences, we define conditional probability.

Definition 15.7. Let A, B be events with $P(B) \neq 0$. The conditional probability $P(A|B)$ is the probability of A assuming B and is given as

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

The idea behind conditional probability is that your new probability set is just B and you are rescaling every probability inside B to get to a sum of one.

Example 15.8. (a) A blue die and a red die are tossed together. What is the probability of getting a sum of 6 if the blue die is showing a 2.

In this case, the event A is " getting a sum of 6". The event B is "the blue die is showing a two'. The event $A \cap B$ is the only option to get 2 in the first die the sum being 6, namely (2,4). Hence, $P(A \cap B) = \frac{1}{36}$, while $P(B) = \frac{1}{6}$. Hence, the probability of getting a sum of 6 when the first die is a 2 is

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{\frac{1}{36}}{\frac{1}{6}} = \frac{1}{6}$$

Notice that in this case, we are computing the probability of the second die being a 4 and this is of course $\frac{1}{6}$.

(b) A blue die and a red die are tossed together. What is the probability of getting an even sum if the blue die is showing a 2?

In this case, the intersection is the event $\{(2,2),(2,4),(2,6)\}$ Therefore,

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{\frac{3}{36}}{\frac{1}{6}} = \frac{3}{6} = \frac{1}{2}$$

Notice that in this case, we are computing the probability of the second die being even, which is of course $\frac{1}{2}$.

Definition 15.9. Two events A, B are said to be independent if and only if

$$P(A|B) = P(A) \Leftrightarrow P(A \cap B) = P(A) \times P(B)$$

From Example 15.8, getting an even sum is independent of getting a 2 on the first die, while getting a sum of 4 is not independent of getting a 2 on the first die.

16. Conditional probability, random variables and expectation, Nov 8

Last class we defined conditional probability $P(A|B)$ as the probability of A assuming B which can be computed as $P(A|B) = \frac{P(A\cap B)}{P(B)}$. There are many occasions in which we are able to compute the probability of A assuming B but that what we are actually interested in is the probability of B assuming A: We will see an example below.

We will look then at random variable and expectation. A random variable is simply a real function on a probability space. The expectation of a random variable plays the role of the average of the function where values are weighed according to their probability.

Those interested in computer science may want to know that probability plays an important role in the field. Randomized algorithms are some times the only way to deal with problems. For some information, please look at

`https://en.wikipedia.org/wiki/Randomized_algorithm`

Example 16.1. In a town in Spain, at the pick of the pandemic, one out of every 50 people was infected with Covid. A rapid test is being given that has 10% false negatives and 2% false positives. If a person's test comes positive, what is the likelihood that he has covid? If another's person test comes negative, what is the likelihood that she has covid?

Let us translate this into the mathematical language we have been using. We are looking at at two events.

- The events C "a person is infected with covid " and its complement NC "a person is not infected with covid ".
- The events PT "a person's covid test is positive" and its complement NT "a person covid test is negative".

A false positive is when a person that is not infected returns a positive test. The likelihood of this happening is $P(PT \mid NC)$.

A false negative is when a person that is infected returns a negative test. The likelihood of this happening is $P(NT \mid C)$.

The given information can be written as

$$P(C) = \frac{1}{50} = 0.02,\ P(NT \mid C) = \frac{10}{100} = 0.1,\ P(PT \mid NC) = \frac{2}{100} = 0.02,$$
$$P(PT \mid C) = 0.9,\ P(NT \mid NC) = 0.98,$$

Where the last two numbers come from the fact that the probability of the complement of an event is 1 minus the probability of the event. What we are trying to compute is the llikelihood of being Covid positive when the test is covid positive $P(C \mid PT)$.

From the definition of conditional probability

$$P(C \mid PT) = \frac{P(C \cap PT)}{P(PT)},\ P(PT \mid C) = \frac{P(C \cap PT)}{P(C)}$$

From the second equation and the data we have

$$P(C \cap PT) = P(PT \mid C)P(C) = 0.9 \times 0.02 = 0.018,$$
$$P(NC \cap PT) = P(PT \mid NC)P(NC) = 0.02 \times 0.98 = 0.0196$$

As $PT = (C \cap PT) \cup (NC \cap PT)$ and this is a disjoint union

$$P(PT) = P(C \cap PT) + P(NC \cap PT)) = 0.018 + 0.0196 = 0.0376$$

Then

$$P(C \mid PT) = \frac{P(C \cap PT)}{P(T)} = \frac{0.018}{0.0376} \cong 0.4787$$

We can similarly compute $P(C \mid NT)$. We already have $P(PT) = 0.0376$. This allows us to compute $P(NT) = 1 - 0.0376 = .9624$. We also need

$$P(C \cap NT) = P(NT \mid C)P(C) = 0.1 \times 0.02 = 0.002,$$

Therefore

$$P(C \mid NT) = \frac{P(C \cap NT)}{P(NT)} = \frac{0.002}{.9624} \cong 0.0207$$

Definition 16.2. A **random variable** is a function $X : S \to \mathbb{R}$ of the sample space of a probability to the set of real numbers. For each real number, the event $X = k$ is the subset of S of elements s such that $X(s) = k$. $P(X = k)$ is the probability of that event.

Example 16.3. (a) When tossing a die, we can define the random variable that assigns to each result the number of dots on the outcome. Then, $P(X = n) = \frac{1}{6}, n = 1, \ldots, 6$.

(b) When tossing two dice, we can define the random variable that assigns to each toss the sum of the numbers that appear on the dice. For example $P(X = 2) = \frac{1}{36}, P(X = 5) = \frac{4}{36}$

Definition 16.4. The expected value of a random variable is the sum of its values multiplied by their probability

$$E(X) = \sum_{s \in S} X(s)P(s)$$

Example 16.5. We compute the expected values for the examples in 16.3

(a) When tossing a die,

$$E(X) = 1 \times \frac{1}{6} + 2 \times \frac{1}{6} + 3 \times \frac{1}{6} + 4 \times \frac{1}{6} + 5 \times \frac{1}{6} + 6 \times \frac{1}{6} = \frac{1+2+3+4+5+6}{6} = \frac{21}{6} = 3.5$$

(b) In Example 15.2, we computed the probability of each of the values of the random variable

$$P(2) = \frac{1}{36} = P(12), P(3) = \frac{2}{36} = P(11), P(4) = \frac{3}{36} = P(10), P(5) = \frac{4}{36} = P(9),$$

$$P(6) = \frac{5}{36} = P(8),\ P(7) = \frac{6}{36}$$

Then,

$$E(X) = \frac{2 + 3 \times 2 + 4 \times 3 + 5 \times 4 + 6 \times 5 + 7 \times 6 + 8 \times 5 + 9 \times 4 + 10 \times 3 + 11 \times 2 + 12 \times 1}{36} = \frac{42}{6} = 7$$

This latter example seems to suggest that the expected value is a sort of middle point.

Definition 16.6. Given two random variables on the same probability set

$$X_1 : S \to \mathbb{R},\ X_2 : S \to \mathbb{R}$$

we can define the following

(a) The sum of random variables $X_1 + X_2 : S \to \mathbb{R}$ assigns to an $s \in S$ $X_1(s) + X_2(s)$.

(b) The product of random variables $X_1X_2 : S \to \mathbb{R}$ assigns to an $s \in S$ $X_1(s)X_2(s)$.

(c) If $c \in \mathbb{R}$, the scalar product cX_1 of the scalar c and a random variable assigns to an $s \in S$ $cX_1(s)$.

Proposition 16.7. *(a) The expected value of the sum of random variables is the sum of the expected values* $E(X_1 + X_2) = E(X_1) + E(X_2)$.
(b) The expected value of the scalar product of a random variables is the product of the scalar and the expected values $E(cX_1) = cE(X_1)$.

Proof. (a) By definition

$$E(X_1) = \sum_{s\in S} X_1(s)P(s),\ E(X_2) = \sum_{s\in S} X_2(s)P(s)$$

Then,

$$E(X_1 + X_2) = \sum_{s\in S}(X_1 + X_2)(s)P(s) = \sum_{s\in S}(X_1(s) + X_2(s))P(s) = E(X_1) + E(X_2)$$

(b) By definition

$$E(X_1) = \sum_{s\in S} X_1(s)P(s))$$

Then,

$$E(cX_1) = \sum_{s\in S}(cX_1)(s)P(s) = \sum_{s\in S} c(X_1(s)P(s)) = cE(X_1)$$

□

Example 16.8. We toss a blue and a red dice. Let X_1 be the random variable that assigns to every toss the number on the blue die. Let X_2 be the random variable that assigns to every toss the number on the red die. Then, $X_1 + X_2$ is the random variable that we discussed in Examples 16.3 16.8 part (b) while X_1 and X_2 are the examples we discussed in part (a). We indeed did obtain that the expected value of $X_1 + X_2$ was the sum of the expected values of X_1, X_2.

Definition 16.9. Two random variables on the same probability set

$$X_1 : S \to \mathbb{R},\ X_2 : S \to \mathbb{R}$$

are said to be independent when

$$P(X_1 = a, X_2 = b) = P(X_1 = a)P(X_2 = b)$$

Example 16.10. The two random variables in 16.8 are indepent

Proposition 16.11. *If* X_1, X_2 *are independent random variables on the same probability space, the expected value of the product of the random variables is the product of the expected values* $E(X_1X_2) = E(X_1)E(X_2)$.

Proof. By definition of expectation

$$E(X_1X_2) = \sum_{s\in S}(X_1X_2)(s)P(s) = \sum_{a\in\mathbb{R}} a \sum_{(X_1X_2)(s)=a} P(s) =$$

$$\sum_{a\in\mathbb{R}} a \sum_{X_1(s)=b, X_2(s)=c,\ bc=a} P(s) = \sum_{a\in\mathbb{R}} a \sum_{b,c\in\mathbb{R},\ bc=a} P(\{X_1(s) = b, X_2(s) = c\})$$

Using now that the two random variables are independent, we have that

$$P(\{X_1(s) = b, X_2(s) = c\}) = P(\{X_1(s) = b\})P(\{X_2(s) = c\})$$

Therefore,

$$E(X_1X_2) = \sum_{a\in\mathbb{R}} a \sum_{b,c\in\mathbb{R},\ bc=a} P(\{X_1(s)=b\})P(\{X_2(s)=c\}) = \sum_{b,c\in\mathbb{R}} bcP(\{X_1(s)=b\})P(\{X_2(s)=c\}) =$$

$$= E(X_1)E(X_2)$$

□

This result is not true if the two random variables are not independent

Example 16.12. (a) Let X_1, X_2 be the random variables that assign to the toss of two dice the number on the first and second die respectively. Let X be the random variable that assigns to each toss, the product of the numbers that appear. Then,

$$E(X) = E(X_1)E(X_2) = \frac{7}{2}\times\frac{7}{2} = \frac{49}{4}$$

Computing the expected value directly is a lot more laborious. The random variable X can take the values

$$1 = 1\times 1,\ 2 = 1\times 2 = 2\times 1,\ 3 = 1\times 3 = 3\times 1,\ 4 = 1\times 4 = 2\times 2 = 4\times 1,$$

$$5 = 1\times 5 = 5\times 1,\ 6 = 1\times 6 = 2\times 3 = 3\times 2 = 6\times 1, 8 = 2\times 4 = 4\times 2, 9 = 3\times 3,$$

$$10 = 2\times 5 = 5\times 2,\ 12 = 2\times 6 = 3\times 4 = 4\times 3 = 6\times 2,\ 15 = 3\times 5 = 5\times 3,\ 16 = 4\times 4,\ 18 = 3\times 6 = 6\times 3,$$

$$20 = 4\times 5 = 5\times 4,\ 24 = 4\times 6 = 6\times 4,\ 25 = 5\times 5,\ 30 = 5\times 6 = 6\times 5,\ 36 = 6\times 6$$

Therefore, we can compute $E(X)$ by first adding the values attained times their frequencies

$$1 + 2\times 2 + 3\times 2 + 4\times 3 +$$
$$+5\times 2 + 6\times 4 + 8\times 2 + 9 +$$
$$+10\times 2 + 12\times 4 + 15\times 2 + 16 + 18\times 2 +$$
$$+20\times 2 + 24\times 2 + 25 + 30\times 2 + 36 = 441$$

Then,

$$E(X) = \frac{441}{36} = \frac{49}{4}$$

(b) Consider the probability space associated to tossing a fair coin. Let X_1, X_2 be the random variables that assign to the toss the number of heads and the number of tails respectively. Then, $E(X_1) = \frac{1}{2}, E(X_1) = \frac{1}{2}$. The product, $X = X_1X_2$ is identically zero. Therefore, $E(X) = 0 \neq E(X_1)E(X_2)$.

Definition 16.13. Given a random variables on a probability space S

$$X_1 : S \to \mathbb{R}$$

we define the **variance** as

$$V(X) = \sum_{x\in S} (X(s) - E(x)))^2 p(s)$$

Example 16.14. (a) When tossing a die, we know that $E(X) = 3.5$. The variance can be seem to be a little less than 3:

$$V(X) = \frac{1}{6}\sum_{i=1}^{6} (i - 3.5))^2 = \frac{35}{12}$$

(b) The random variable X_1 takes the value -1 with probability $\frac{1}{3}$, the value 0 with probability $\frac{1}{3}$ and the value 1 with probability $\frac{1}{3}$. The expected value is 0. The variance is then

$$V(X_1) = \frac{1}{3}[(-1-0)^2 + (0-0)^2 + (1-0)^2] = \frac{2}{3}$$

(c) The random variable X_2 takes the value -2 with probability $\frac{1}{3}$, the value 0 with probability $\frac{1}{3}$ and the value 2 with probability $\frac{1}{3}$. The expected value is 0. The variance is then

$$V(X_2) = \frac{1}{3}[(-2-0)^2 + (0-0)^2 + (2-0)^2] = \frac{8}{3}$$

(d) The random variable X_3 takes the value -2 with probability $\frac{1}{4}$, the value 0 with probability $\frac{1}{2}$ and the value 2 with probability $\frac{1}{4}$. The expected value is 0. The variance is then

$$V(X_2) = \frac{1}{4}(-2-0)^2 + \frac{1}{2}(0-0)^2 + \frac{1}{4}(2-0)^2] = 4$$

We can see from Examples 16.14 how the variance measures how close together the outputs of the random variable are.

17. Introduction to graphs, November 15

In this section, we introduce the study of graphs. Graphs will allow us to find solutions to problems that a curious person could ask and also to take a look at a variety of more profound mathematical problems, particularly in the area of Topology. Graphs also have a wide application to various areas of science and in particular to computer science (see `http://www.cs.xu.edu/csci390/12s/IJEST10-02-09-124.pdf` for more on this).

Definition 17.1. A **graph** is a triple (V, E, f) where G is a set called the set of **vertices**, E is a set called the set of **edges**, and f is a function with domain E and codomain the set of subsets of unordered pairs of elements of V that we can write as the set of cosets of $V \times V$ by the equivalence relation that identifies (a, b) with (b, a), $f : E \to V \times V/\sim$.

We will only consider finite graphs, meaning that both V, E are finite sets. We think of graphs as a collection of points, the vertices, together with a collection of segments (the edges) each joining two points.

Example 17.2. (a) Consider a graph such that

$$V = \{a, b, c, d\}, E = \{e_1, e_2, e_3.e_4, e_5\},$$

$$f(e_1) = \{a, d\}, f(e_2) = \{a, d\}, f(e_3) = \{a, b\}, f(e_4) = \{b, d\}, f(e_5) = \{c, c\}$$

This is the left graph shown in Figure 17

(b) Consider a graph such that

$$V = \{a, b, c, d\}, E = \{e_1, e_2, e_3.\},$$

$$f(e_1) = \{a, d\}, f(e_2) = \{a, b\}, f(e_3) = \{b, c\}$$

This is the right graph shown in Figure 17

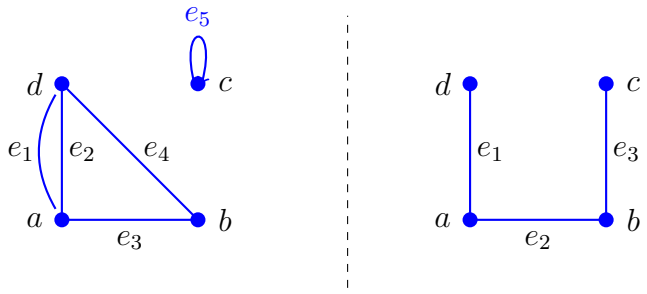


Figure 17. Two examples of graphs with 4 vertices a, b, c, d and 5 and 3 edges respectively

Definition 17.3. An edge e is said to be **incident** with a vertex a if $a \in f(e)$. Two vertices $a, b \in V$ are **adjacent** or **neighbors** if there is some edge $e \in E$ such that $f(e) = \{a, b\}$. Then, we will say that e is incident with a, b and that a, b are the **end points** of e.

A **loop** in a graph is an edge e such that $f(e) = \{a, a\}$ for some $a \in V$.

Given two vertices $a, b \in V$, we say there are **multi-edges** between a and b if there are at least two edges e, e' such that $f(e) = f(e') = \{a, b\}$.

A graph is **simple** if it does not have loops or multi-edges.

Example 17.4. (a) In the first graph in Example 17.2, e_1, e_2 are multi-edges between a, b. Also, e_5 is a loop. This graph is not simple.
(b) In the second graph in Example 17.2, a, d are adjacent while c, d are not. This graph is simple.

Definition 17.5. The **degree** of a vertex in a graph is the number of edges incident with that vertex where a loop is counted twice

Example 17.6. (a) In the first graph in Example 17.2,

$$\deg(a) = 3,\ \deg(b) = 2,\ \deg(c) = 2,\ \deg(d) = 3$$

(b) In the second graph in Example 17.2,

$$\deg(a) = 2,\ \deg(b) = 2,\ \deg(c) = 1,\ \deg(d) = 1$$

Proposition 17.7. *The sum of the degrees of the vertices in a graph is twice the number of edges.*

Proof. Each edge which is not a loop contributes twice to each of the degrees of its end points with a loop contributing twice to its unique end point. □

Definition 17.8. Given two graphs $(V, E, f), (V', E', f')$, a morphism from the first graph to the second one is a pair of functions

$$g_V : V \to V',\ g_E : E \to E'$$

preserving incidences, that is $f(e) = \{a, b\}$, then $f'(g_E(e)) = \{g_V(a), g_V(b)\}$. Equivalently, we have a commutative diagram of functions

$$\begin{array}{ccc} E & \xrightarrow{f} & V \times V/\sim \\ g_E \downarrow & & \downarrow g_V \times g_V \\ E' & \xrightarrow{f'} & V' \times V'/\sim \end{array}$$

Definition 17.9. Given two graphs $(V, E, f), (V', E', f')$, we will say they are isomorphic if there are bijections between the set of vertices of the two and the set of edges of the two preserving incidences, that is

$$g_V : V \to V',\ g_E : E \to E'$$

satisfies that if $f(e) = \{a, b\}$, then $f'(g_E(e)) = \{g_V(a), g_V(b)\}$.

Proposition 17.10. *Let $(V, E, f), (V', E', f')$ be two graphs and (g_V, g_E) a morphism between the two.*

(a) Isomorphisms of graphs preserve degrees of vertices, that is $\forall a \in V, \deg a = \deg g_V(a)$ where the first degree is computed in the graph (V, E, f), and the second in (V', E', f').
(b) Isomorphisms of graphs preserve adjacency, that is $\forall a, b \in V$ if a is adjacent to b, then $g_V(a)$ is adjacent to $g_V(b)$.
(c) Isomorphisms of graphs preserve loops and multi-edges

Proof. (a) The degree of a vertex $v \in V$ is the number of edges $e \in E$ such that $v \in f(e)$ with v counted with multiplicity two if v is an edge whose image is the pair $\{v, v\}$. From the definition of isomorphism, if $v \in f(e)$, then $g_V(v) \in g_E(e)$ and it appears with multiplicity two if e and therefore $g_E(e)$ is a loop. Therefore, the degree of the vertex and of its image is the same

(b) If $a, b \in V$ with a adjacent to b in (V, E, f), then there exists $e \in E$ such that $f(e) = \{a, b\}$. From the definition of isomorphism, $f'(g_E(e)) = \{g_V(a), g_V(b)\}$. Therefore, $g_V(a), g_V(b)$ are also adjacent.

(c) If $a, b \in V$ are vertices of a multiedge, then there exists $e_1, e_2 \in E, e_1 \neq e_2$ such that $f(e_1) = \{a, b\} = f(e_2)$. Then, $f'(g_E(e_1)) = \{g_V(a), g_V(b)\} = f'(g_E(e_2))$. Therefore, $g_V(a), g_V(b)$ are vertices of a multiedge.

Something similar works for a loop.

□

Example 17.11. (a) Consider the two graphs in Figure a. We can define a bijection that preserves edges as follows

$$g_V(a) = 1,\ g_V(b) = 3,\ g_V(a) = 1,\ g_V(c) = 2,\ g_V(d) = 4$$

The edge e_1 maps to the edge with vertices $1, 4$, the edge e_2 maps to the edge with vertices $1, 3$, the edge e_3 maps to the edge with vertices $2, 3$, the edge e_4 maps to the edge with vertices $2, 4$,

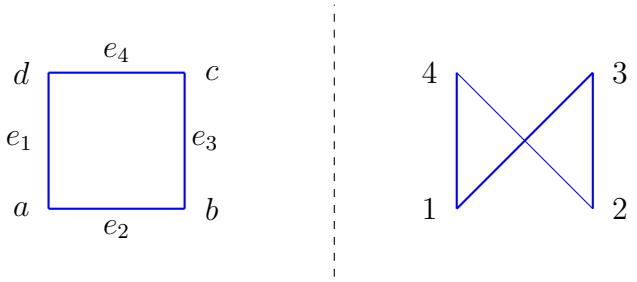
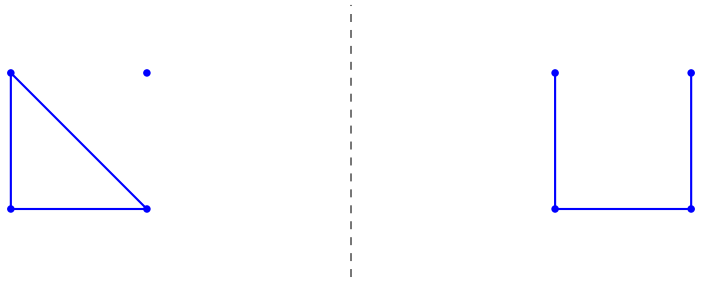


FIGURE 18. Two isomorphic graphs.

(b) The two graphs below, both have 4 vertices and 3 edges but they are not isomorphic as one has a vertex of degree 0 and the other doesn't.



(c) We showed that if two graphs are isomorphic, corresponding vertices have the same degree. Showing that they are not isomorphic may be more subtle. Looking at the two graphs in Figure b, we can check that in the first graph, vertex a has degree 3, vertices b, d have degree 2 and vertex c has degree 1.

In the second graph, vertex D have degree 3, vertices A, B have degree 2 and vertex C has degree 1.

Still, they are not isomorphic for a number of reasons. The first one has a multi-edge, the second does not. The only vertex c of degree one in the first graph is adjacent to

FIGURE 19. Two examples of graphs with with the same number of vertices of the same degree but not isomorphic.

a vertex b of degree 2 , while the only vertex C of degree one in the second graph is adjacent to a vertex D of degree 3.

In the first graph, vertices b, e have degree 3, vertices a, f have degree 2 and vertices c, d have degree 1.

In the second graph, vertices B, F have degree 3, vertices A, E have degree 2 and vertices C, D have degree 1.

An isomorphism between the two graphs should send the pair of vertices $\{c, d\}$ to the pair of vertices $\{C, D\}$. But the vertices C, D are adjacent. The edge that connects them should be the image of an edge connecting c, d. But no such edge exists. So no isomorphism is possible.

(d) The two graphs are not isomorphic. If they were, g which is a vertex of degree two should correspond with a vertex of degree two on the right hand side graph. Therefore, it should correspond to either B, D, F or H, But g is adjacent to two vertices of degree two while each of B, D, F, H are adjacent to a vertex of degree two and a vertex of degree three. Hence, no isomorphism can exist.

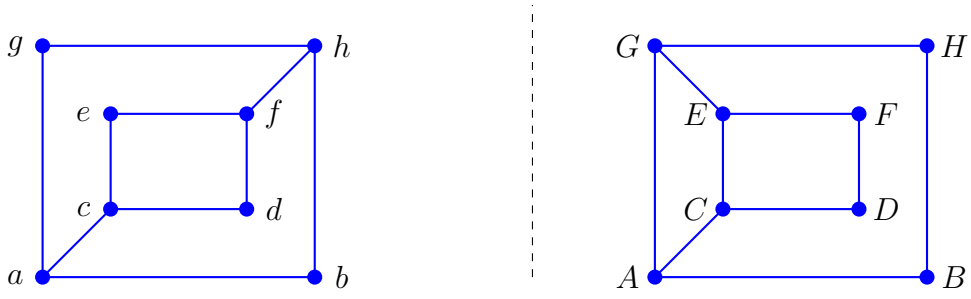


FIGURE 20. More examples of non-isomorphic graphs.

For more examples, please see the quiz answers.

18. More graphs and subgraphs, November 17.

Recall that we defined a morphism from $G = (V, E, f)$ to $G' = (V', E', f')$, as a pair of functions $g_V : V \to V'$, $g_E : E \to E$ that preserves incidence. We will say that G is a subgraph of G' when both functions are one to one, meaning that the set of vertices of G is a subset of the set of vertices of G' and the of edges of G is a subset of the set of edges of G'.

Definition 18.1. The graph $G = (V, E, f)$ is a subgraph of $G' = (V', E', f')$, if there is a pair of one-to -one functions

$$g_V : V \to V', \ g_E : E \to E'$$

preserving incidences.

We can construct a subgraph of G' by keeping the same set of vertices and removing some edges. On the other hand, if we want to remove vertices, we need to remove all the edges that join them.

Definition 18.2. Recall that the **complete graph** K_n on n vertices is a simple graph with n vertices and one edge joining any pair of vertices.

A **bipartite graph** G is a graph whose set of vertices can be written as the disjoint union of two sets $V = V_1 \cup V_2$ and edges join one vertex in V_1 to a vertex in V_2 (but there are no edges among vertices of V_1 or vertices of V_2).

The **complete bipartite graph** $K_{m,n}$ is a graph with set of vertices $V = V_1 \cup V_2$ where V_1 has m elements, V_2 n elements and there is one edge joining every vertex in V_1 to every vertex in V_2 (but no edges among vertices of V_1 or vertices of V_2).

Example 18.3. (a) The picture below shows K_2, K_3, K_4.

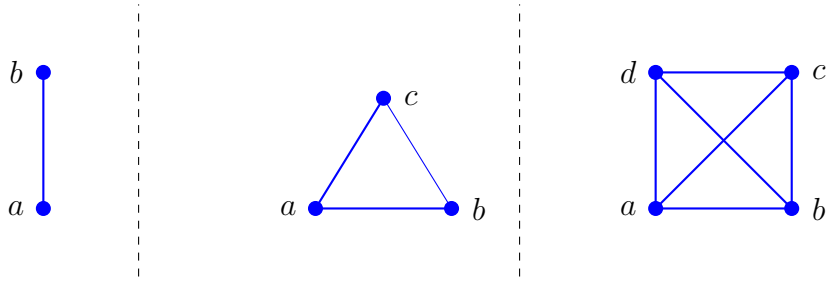


Figure 21. K_2, K_3, K_4.

(b) We sketch below the complete bipartite graph $K_{2,3}$.

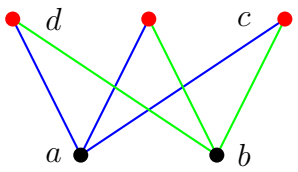


Figure 22. $K_{2,3}$.

Proposition 18.4. *(a) The complete graph K_n has n vertices each of degree $n-1$, and $\binom{n}{2}$ edges.*
(b) Every simple graph with n vertices is a subgraph of K_n.
(c) The complete bipartite graph $K_{m,n}$ has by definition $m+n$ vertices. The vertices in V_1 have degree n, the vertices in V_2 have degree m, and there are $m \times n$ edges.
(d) Every simple bipartite graph of type (m,n) is a subgraph of $K_{m,n}$.

Proof. (a) By definition K_n has n vertices. As there is one edge precisely for every two vertices, there are $\binom{n}{2}$ edges. As there is an edge from every vertex to every other vertex, each vertex has degree $n-1$.
(b) A simple graph has at most one edge between every pair of vertices. As K_n has n vertices and all possible edges that a simple graph can have, we can obtain every other simple graph with n vertices by removing edges from K_n.
(c) The complete bipartite graph $K_{m,n}$ has by definition $m+n$ vertices. There are m vertices in V_1 and each of them has one edge for each of the n vertices in V_2. Therefore, each vertex in V_1 has degree n and similarly each vertex in V_2 has degree m. and there are $m \times n$ edges in all.
(d) As $K_{m,n}$ has all the edges it can possibly have while staying bipartite and simple simple, every bipartite graph of type (m,n) can be obtained from $K_{m,n}$ by removing edges and therefore is a subgraph of $K_{m,n}$.

□

Example 18.5. We can obtain $K_{2,3}$ from K_5 by removing the 4 edges, the one joining the two vertices of the group of 2 and the 3 joining the vertices of the group of 3.

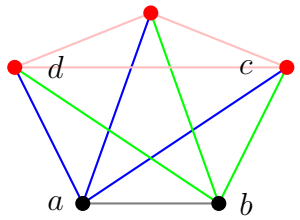


FIGURE 23. Going from K_5 to $K_{2,3}$ by removing edges.

Definition 18.6. If $G=(V,E,f)$ is a graph, a **clique** is a subgraph of G such that there is an edge between every two vertices.

The **clique number** $\omega(G)$ is the number of vertices in the largest clique in G. In other words,

$$\omega(G) = \max\{n | K_n \text{ subgraph of } G\}$$

An **independent set** is a subgraph of G such that there are no edges between any two vertices of the set.

The **independence number** $\alpha(G)$ is the number of vertices in the largest independent set in G.

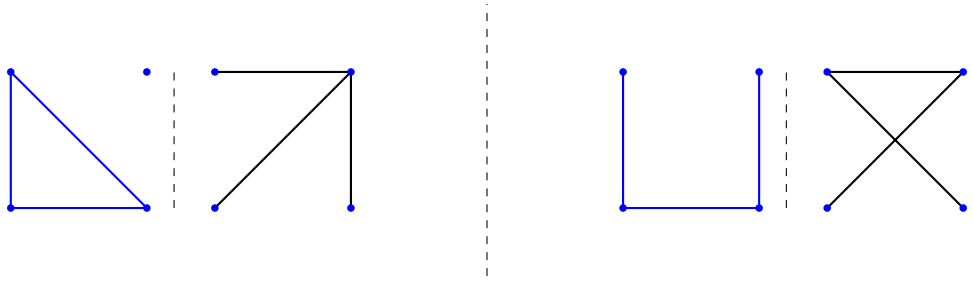
Example 18.7. (a) The clique number of K_n is n, the independence number is 1.
(b) The clique number of $K_{n,m}$ is 2: take a vertex in each of the two sets of the partition, then by definition of the complete bipartite graph, there is an edge between the two.

On the other hand, for any set of 3 or more vertices, by the pigeon hole principle, there are at least two on one of the two sets of vertices of the partition and therefore, no edge between the two.

The independence number of of $K_{n,m}$ is the largest of n, m: each of the two sets of vertices of the partition are independent. On the other hand, if $k > \max\{n, m\}$, any set with k or more vertices contains vertices from both sets and therefore contains at least one edge between two vertices.

Definition 18.8. If $G = (V, E, f)$ is a simple graph with n vertices, the **complement of G** is the simple graph $\bar{G} = (V, (V \times V/\sim) - E, \bar{f})$ with the same set of vertices as G and the complementary set of edges (in the natural identification of G with a subgraph of K_n).

Example 18.9. (a) Here is an example of two pairs of a graph and their complement.



(b) The complement of K_n is a graph with n vertices and the empty set of edges.

(c) The complement of $K_{m,n}$ is a graph which is a disjoint union of a K_m and a K_n. Looking at the number of edges of each of these graphs, we have

$$|E(K_{m+n})| = |E(K_{m,n})| + |\bar{E}(K_{m,n})| = |E(K_m)| + |E(K_n)| + |E(K_{m,n})|$$

This provides a combinatorial proof of the identity

$$\binom{m+n}{2} = \binom{m}{2} + \binom{n}{2} + mn$$

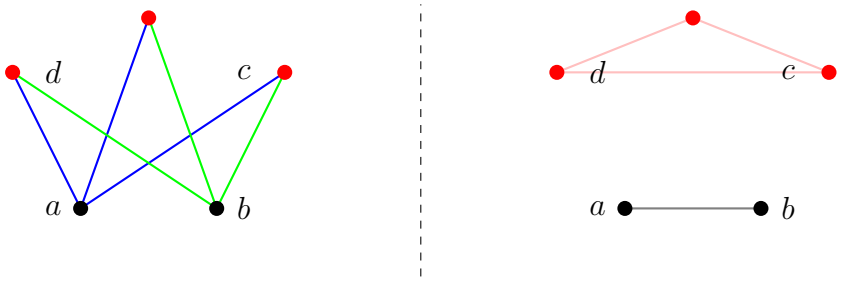


FIGURE 24. The graph $K_{2,3}$ and its complement.

Proposition 18.10. *Let $G = (V, E, f)$ be a simple graph,*

(a) If $G_1 = (V_1, E_1, f_1)$ a subgraph of G that is a clique, then $G_1' = (V_1, \emptyset,)$ is an independent set of the complement graph $\bar{G}$.

(b) If $G_1 = (V_1, \emptyset,)$ is an independent set of G, then $G_1' = (V_1, E(K_{V_1}), f(K_{V_1}))$ is a clique of the complement graph $\bar{G}$, where K_{V_1} denotes the complete graph on the vertices of V_1.
(c) The clique and independence numbers of G and its complement are switched

$$\omega(G) = \alpha(\bar{G}),\ \alpha(G) = \omega(\bar{G})$$

Proof. (a) If $G_1 = (V_1, E_1, f_1)$ a subgraph of G that is a clique, then for every two vertices in V_1,the edge that joins them is in $E_1 \subseteq E$. Therefore, this edge needs to be removed when constructing the complementary graph. It follows that there are no edges among the vertices of V_1 in $\bar{G}$. Therefore $G_1' = (V_1, \emptyset,)$ is an independent set of the complement graph $\bar{G}$.

(b) If $G_1 = (V_1, \emptyset,)$ is an independent set of G, then there are no edges among these vertices in G. Therefore, for every pair of vertices in V_1, we need to add one edge in the construction of the complement. It follows that K_{V_1} is a subgraph of $\bar{G}$, where K_{V_1} denotes the complete graph on the vertices of V_1.

(c) From (a) and (b),

$$\alpha(\bar{G}) \geq \omega(G),\ \omega(\bar{G}) \geq \alpha(G)$$

As the complement of the complement of a graph is the original graph

$$\alpha(G) \geq \omega(\bar{G}),\ \omega(G) \geq \alpha(\bar{G})$$

Therefore, we have equality.

□

Proposition 18.11. *If $G = (V, E, f)$ is a simple graph with $n \geq 6$ vertices, then either $\alpha(G) \geq 3$ or $\omega(G) \geq 3$*

Proof. Assume first that at least one vertex a of the graph has degree 3 or more. Then, there are edges from a to b, c, d. If there is at least one edge between a pair among b, c, d, then, this pair along with a will form a clique, and therefore $\omega(G) \geq 3$. If there is no edge between any pair among b, c, d, then, this set is independent and therefore $\alpha(G) \geq 3$.

Assume then that the degree d of a vertex is at most two. Then, in the complementary graph, the degree of that vertex is $n-1-d \geq 6-1-2 = 3$. We can then apply the previous argument to $\bar{G}$ and obtain that either $\omega(\bar{G}) \geq 3$ or $\alpha(\bar{G}) \geq 3$. As $\alpha(G) = \omega(\bar{G}), \omega(G) = \alpha(\bar{G})$, this proves the result. □

This statement is usually stated in the more colloquial form: in a group of 6 people were every two are either collaborators or competitors, there are at least 3 mutual collaborators or three mutual competitors.

19. Paths, November 22.

Interesting questions, from diagnostic in computer networks, to finding the cheapest air fare between two destinations, can be formulated by considering paths that join vertices of a graph. Let us start by defining what we mean by a path in a graph.

Definition 19.1. Given a graph $G = (V, E, f)$, a **path** in G is a finite ordered sequence of vertices and edges

$$P = (v_0, e_1, v_1, e_2, v_2, \ldots, v_{n-1}, e_n, v_n),\ v_0, \ldots, v_n \in V,\ e_1, \ldots, e_n \in E,\ f(e_i) = \{v_{i-1}, v_i\}$$

The path is said to **join** the vertices v_0, v_n or to be a path **from** v_0 **to** v_n. The path is said to **traverse** the edges $e_1, e_2, \ldots, e_n$.

A path is **simple** if the edges are all different. A path is **a circuit** if $v_0 = v_n$.

Note that if a graph is simple, a path is determined by the sequence of vertices, there is no need to give the edges, as there is at most one edge between two vertices. Still, vertices cannot be chosen at random, there needs to be an edge between two consecutive vertices.

Example 19.2. (a) In the left of Figure 25, $(d, e_1, a, e_3, b, e_5, c, e_6, d, e_2, a)$ is a simple path.

The path $(d, e_1, a, e_3, b, e_5, c, e_6, d, e_1, a)$ is not simple as the edge e_1 is used twice.

The path $(d, e_1, a, e_3, b, e_4, d)$ is a simple circuit as all edges are different and the starting and ending vertices are the same.

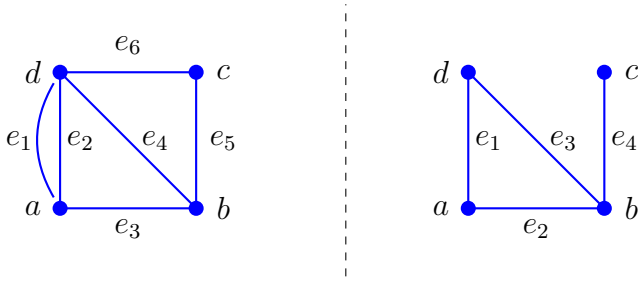


Figure 25. Paths in graphs

(b) In the right picture, we can determine a path by just giving the vertices, for example, d, a, b, d determines the path $(d, e_1, a, e_2, b, e_3, d)$. On the other hand, a, b, c, a does not determine any path, as there is no edge e with $f(e) = \{a, c\}$.

On the left picture, d, a, b, d does not determine a unique path as there are two possible edges from d to a, so both $(d, e_1, a, e_3, b, e_4, d)$ and $(d, e_2, a, e_3, b, e_4, d)$ are paths with the given set of vertices in the given order.

For two vertices, a, b, we said that there is a path between a and b, if there is a path with first vertex a and last vertex b. We will check that with our definition of graph, the order of the vertices does not matter and also that there is a path between intermediate vertices.

Proposition 19.3. *Let $G = (V, E, f)$ be a graph, $a, b \in V$.*

(a) If there is a path from a to b, then there is also a simple path from a to b.

(b) If there is a path from a to b, then there is also a path from b to a.

(c) If there is a path $P = (v_0, e_1, v_1, e_2, v_2, \ldots, v_{n-1}, e_n, v_n)$ with $a, b \in \{v_0, \ldots, v_n\}$, then there is a path from a to b.

Proof. (a) Assume that there is at least one path from a to b. Choose the path with the shortest number of edges $P = (a = v_0, e_1, v_1, e_2, v_2, \ldots, v_{n-1}, e_n, v_n = b)$ from a to b. We claim that this path is simple. If ti were not, then there is a pair of edges $e_i, e_j, i < j$ with $e_i = e_j$. As the two edges e_i, e_j are the same, their end points are also the same and therefore $\{v_{i-1}, v_i\} = \{v_{j-1}, v_j\}$.

If $v_{i-1} = v_{j-1}, v_i = v_j,$ then $P = (a = v_0, e_1, v_1, \ldots, v_{i-1}, e_i, v_i = v_j, e_{j+1}, \ldots, v_{n-1}, e_n, v_n = b)$ is also a path from a to b and it is shorter, contradicting our initial choice of path.

If $v_{i-1} = v_j, v_i = v_{j-1}$ then $P = (a = v_0, e_1, v_1, \ldots, v_{i-1} = v_j, e_{j+1}, \ldots, v_{n-1}, e_n, v_n = b)$

Hence, the initial shortest path was simple.

(b) If there is a path from $P = (a = v_0, e_1, v_1, e_2, v_2, \ldots, v_{n-1}, e_n, v_n = b)$ from a to b, then

$$P' = (b = v_n, e_n, v_{n-1}, e_{n-1}, \ldots, v_2, e_2, v_1, e_1, v_0 = a)$$

is also a path and goes from b to a.

(c) If there is a path $P = (v_0, e_1, v_1, e_2, v_2, \ldots, v_{n-1}, e_n, v_n)$ with $a = v_i, b = v_j, i < j$, then

$$P' = (a = v_i, e_{i+1}, v_{i+1}, \ldots, v_{j-1}, e_j, v_j = b)$$

is a path from a to b. If $a = v_i, b = v_j, i > j$, the roes of a, b can be reversed and there is a path from b to a. Then, part (b) above shows that there is a path from a to b.

□

We will define a relation among vertices that tell us when two vertices can be connected by a path

Proposition 19.4. *Let $G = (V, E, f)$ be a graph, $a, b \in V$. We define the relation $a \sim b$ if and only if there is a path from a to b. Then $\sim$ is an equivalence relation in the set of vertices. The equivalence classes partition the vertices in subsets in such a way that edges are vertices among only one of these subsets. Therefore, we can view the graph as a disjoint union of subgraphs called the* **connected components**.

Proof. We first check that $\sim$ is an equivalence relation

- Given $v \in V$, from our definition of path with $n = 0$, $P = (v)$ is a path from v to v. Hence, $v \sim v$.
- the relation is symmetric from Proposition 19.3 part(b).
- the relation is transitive: if $a \sim b$ and $b \sim c$, then there exist paths

$$P = (a = v_0, e_1, v_1, \ldots, v_{n-1}, e_n, v_n = b),\ P' = (b = v'_0, e'_1, v'_1, \ldots, v'_{n'-1}, e'_{n'}, v'_{n'} = c).$$

Then we can construct a path from a to c as

$$P'' = (a = v_0, e_1, v_1, \ldots, v_{n-1}, e_n, v_n = b, e'_1, v'_1, \ldots, v'_{n'-1}, e'_{n'}, v'_{n'} = c).$$

Therefore, $a \sim c$

Every equivalence relation on a set divides the set into equivalence classes that cover the set and are disjoint. Therefore, we can write $V = V_1 \cup \cdots \cup V_k$ where each V_k is one of the equivalence classes. Let E_i be the set of edges such that they have vertices in the set V_i, that is

$$E_j = \{e \in E | f(e) \subseteq V_i\}.$$

We claim that $E = E_1 \cup \cdots \cup E_k$ To prove the claim, take $e \in E$ and let $f(e) = \{v, v'\}$. Then $P = (v, e, v')$ is a path from v to v'. Hence, $v \sim v'$ and therefore the equivalence classes of v and v' by the relation are the same. Therefore, $\exists j, v \in V_j, v' \in V_j$. Then, from the definition of $E_j, e \in E_j$. As every element in E is in one E_j and from definition the E_j are disjoint, E is the disjoint union of the E_j.

Therefore the graph is the disjoint union of disjoint graphs. □

Oriented graphs can be defined similarly to non-oriented graphs except that the pair of vertices of every edge are ordered. In that situation, one should think of a beginning vertex and an end vertex instead of a pair of vertices. For oriented graphs, (b) in Proposition 19.3 is no longer true and paths and connected components should be defined in a different way.

20. Euler Graphs, November 29

This section has a historical background. In the city of Köninsberg there was a river that divided into two branches and also had an island in the middle. There were four pieces of land, namely the right and left river banks, the island and the piece separated by the two branches. Several bridges connected the various pieces. Legend has it that a common pass time was to try to go through the seven bridges once and returning home.

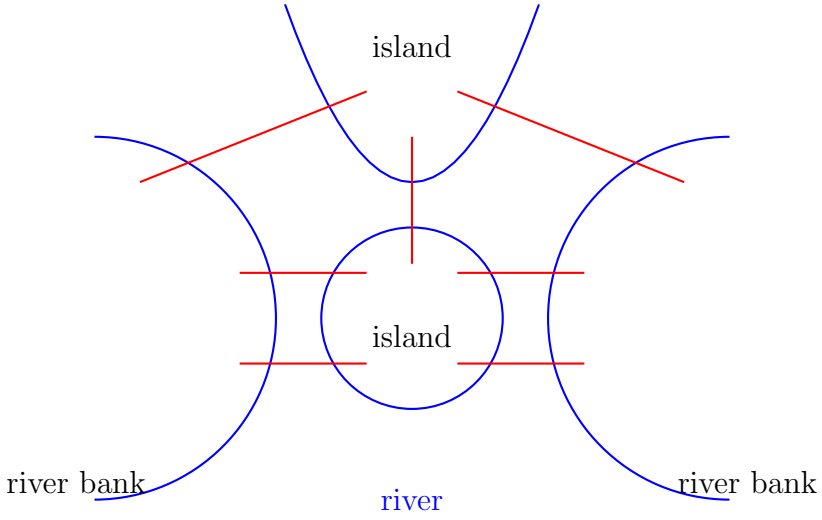


Figure 26. The seven red bridges connect river banks and islands

Euler translated the situation into a graph theory question and then showed it had no answer. In fact, his work trying to solve this problem is regarded as the introduction of graph theory and combinatorics, a theory that has proved extremely useful in the solution of far more relevant problems than the ones that originated it

`https://en.wikipedia.org/wiki/Seven_Bridges_of_K%C3%B6nigsberg`

Euler constructed a graph with a vertex for each piece of land and edges for the bridges. We get a graph with vertices l, r, i, u corresponding respectively to the left and right river banks, the island and upper island. We have edges for any bridge with b_1, b_2 connecting the left bank to the island, b_3 connecting the left bank to the upper island, b_5, b_6 connecting the right bank to the island, b_7 connecting the right bank to the upper island and b_4 connecting the two islands.

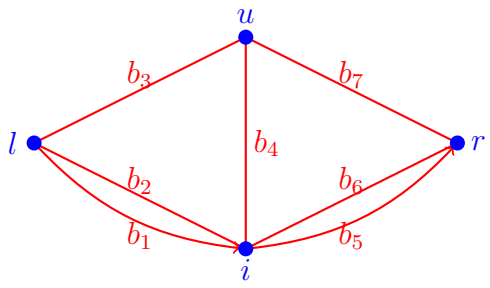


Figure 27. A graph representing the Köningsberg bridges.

With this translation, the question we want to answer is the following:

Question 20.1. Given a not necessarily simple graph, when is there a simple closed path containing all edges.?

When we talk about a simple path, we mean that we do not repeat edges (even if the graph itself may not be simple and can have multi-edges). When we talk about a closed path, we mean that it begins and ends with the same vertex.

First of all, we are only interested in connected graphs. Any path is completely contained in a connected component. If there is a path containing all edges, then there is one connected component containing all edges and perhaps a few more consisting of one vertex each with no edges.

Definition 20.1. We will say that a connected graph has **an Euler circuit** if there is a simple closed path (a circuit) containing all edges of the graph. We will also say that the graph is **Eulerian**.

We will say that a graph has **an Euler path** if there is a simple non-closed path (starting and ending at different points) containing all edges of the graph.

We notice that because, when following a path, we need to get into every vertex as many times as we get out and we should be using every edge at that vertex in the process, the degree at every vertex must be even, if we are considering a closed path. If we consider a non-closed path, the degree at every vertex must be even except at the beginning and end points where it must be odd.

We want to show the converse..

Proposition 20.2. *Given a connected graph $G = (V, E, f)$, the path has an Euler circuit if and only if every vertex has even degree. In this situation, the start (and therefore ending point) can be any vertex of our choosing.*

Proof. We already proved the only if part. Before we prove the if part, a useful remark:

If every vertex of a graph has even degree, we claim that every maximal simple path is closed. By a maximal simple path we mean a path that cannot be made any longer while keeping it simple. A maximal simple path only needs to stop when we reach a vertex where all edges have been used. If we get in and out of a vertex, we decrease the number of unused edges by two. If the degree is even, we will only need to stop at the initial vertex.

Assume now that in the graph G, every vertex has even degree and take a maximal simple path starting at a vertex of our choosing. By the above remark, this path is closed. If all edges have not yet been used, consider the graph obtained by removing all used edges. We will be removing an even degree from the degree of each vertex. Therefore, the degrees of the vertices with the left over edges is still even. As the whole graph is connected, the remaining edges must intersect the previously used for the path.

Start then a path at one vertex of the old path at which there are left over edges. Form a path until we need to stop, which will happen only when we get back at the initial vertex. Then, the newly formed path can be added to the old path inserting it at the vertex where we started. This contradict the maximality of the original path. Hence, a maximal path contains all edges. □

Proposition 20.3. *Given a connected graph $G = (V, E, f)$, the graph has an Euler path if and only if every vertex except for two have even order and then the path starts and ends at the vertices of odd degree*

Proof. Again, we already proved the only if part.

Assume now that two of the vertices of G have odd degree and the rest have even degree. Start a path at one of the two vertices of odd degree. The path will only stop if we reach the other odd degree vertex. Removing this path from the initial graph, we are left with a graph in which all vertices have now even degree. We can then apply the same trick as in the case of all even degrees to produce a longer path.

For an alternative proof: add to the graph an edge joining the two odd degree vertices. In the new graph, every vertex has even degree. Therefore, there is an Euler circuit in which the added edge e appears exactly once:

$$P = (v_0, e_1, v_1, e_2, v_2, \ldots, v_{i-1}, e_i, v_i, \ldots, v_{n-1}, e_n, v_n),\ e_i = e,\ \{e_1, \ldots, e_n\} = E, v_0 = v_n$$

Then,

$$P' = (v_i, e_{i+1}, v_{i+1}, \ldots, v_{n-1}, e_n, v_n = v_0, e_1, v_1, e_2, v_2, \ldots, v_{i-1})$$

is a path that uses all edges of the old graph exactly once, does not use the added edge and begins and ends at the odd degree vertices. Therefore, it satisfies all the stated conditions. □

It is worth noticing that the proof leads to a construction of an Euler path or Euler circuit for a qualifying graph.

Example 20.4. (a) In the Köninsberg bridge example, the degrees of the vertices are $3, 3, 3, 5$ so there are no Euler paths or circuits, as there are five vertices of odd degree.

(b) Consider the graph K_5. As the degree of every vertex is 4, there is an Euler circuit. Let us try to construct one starting at the vertex a using the strategy of the proof. This graph is simple, an edge is completely determined by its end points, for example $e_{a,b}$ can denote the unique edge from vertex a to vertex b. So, we can determine a path by just giving the vertices it travels trough.

Consider then the path $P = (a, e_{a,b}, b, e_{b,c}, c, e_{a,c}, a, e_{a,d}, d, e_{d,e}, e, e_{a,e}, a)$. We cannot proceed now, as there are no edges left at a. The degree of the graph formed by the left over vertices is zero at a and two at the remaining vertices. We can form a path starting for instance at b $P' = (b, e_{b,d}, d, e_{c,d}, c, e_{c,e}, e, e_{b,e}, b)$. Then, we can insert this path in P at b to obtain the following Euler path

$$P'' = (a, e_{a,b}, b, , e_{b,d}, d, e_{c,d}, c, e_{c,e}, e, e_{b,e}, b, e_{b,c}, c, e_{a,c}, a, e_{a,d}, d, e_{d,e}, e, e_{a,e}, a).$$

(c) Another example of an eulerian graph, this time with multiple edges is depicted below. Starting at node b,we create the path

$$P = (b, e_{12}, c, e_{10}, a, e_{11}, b)$$

We cannot continue this path, so we start over with the left over vertices starting at a and we create the path

$$P' = (a, e_1, d, e_2, a, e_3, d, e_4, a)$$

Again, we are corned up with no escape route. We start over at c and create the path

$$P'' = (c, e_5, f, e_9, d, e_7, e, e_8, f, e_6, c)$$

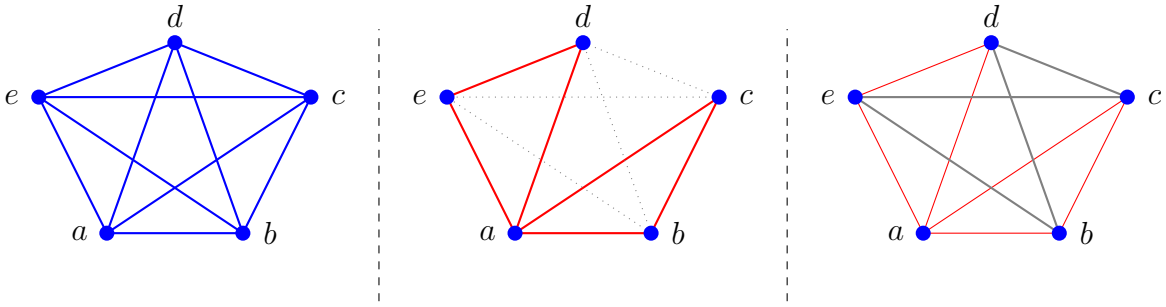


FIGURE 28. The graph K_5,the first attempt at an Euler path, and the leftover path .

Now, we used up all edges. Putting together all paths, we obtain the eulerian path

$$\bar{P} = (b, e_{12}, c, e_5, f, e_9, d, e_7, e, e_8, f, e_6, c, e_{10}, a, e_1, d, e_2, a, e_3, d, e_4, a, e_{11}, b)$$

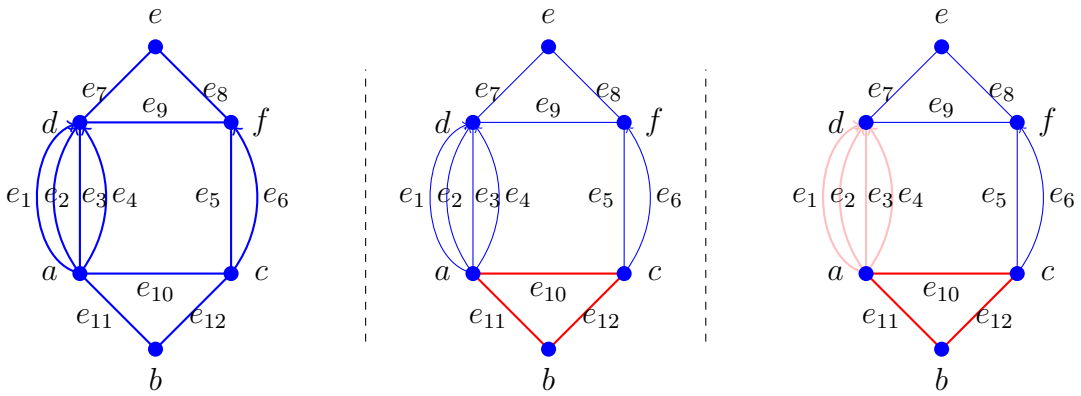


FIGURE 29. Building an eulerian path in a multigraph

21. Trees, December 1

A simple closed path of length n is often called an n-cycle. An n-cycle is a graph on its own and any two n-cycles are isomorphic.

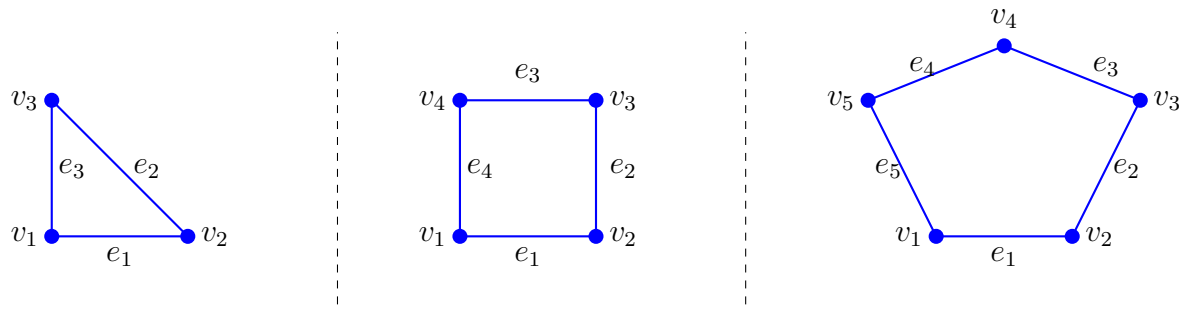


FIGURE 30. The graphs C_3, C_4, C_5

Every graph has trivial closed paths. By a trivial closed path we mean a path that covers a few edges and then covers the same edges in the opposite direction just going back and forth.

We now want to focus on graphs that do not have non-trivial closed paths. A multi-edge e_1, e_2 joining two vertices u, v creates a non-trivial closed circuit u, e_1, v, e_2, u, We want to look at graphs that do not have any loops other than the trivial ones, so we will exclude multi-edges and loops.

Definition 21.1. A **tree** is a connected simple graph that does not contain n-cycles (for any n).

A **forest** is a not necessarily connected simple graph that does not contain any n-cycles.. Equivalently, a forest is a graph whose connected components are trees.

Example 21.2. The left graph in Figure 31 is not a tree as the edges e_1, e_2, e_3 form a circuit. The other two graphs are trees as they do not containn any cycles.

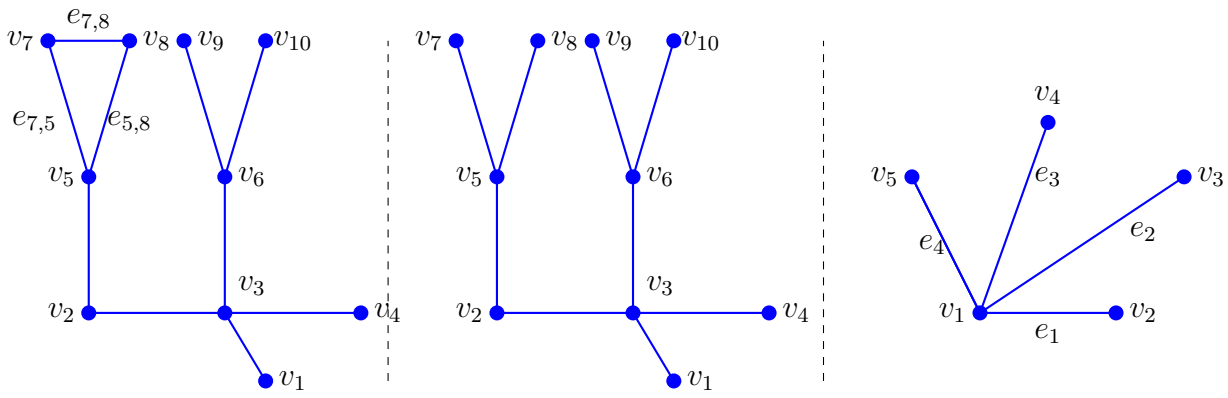


FIGURE 31. The first graph is not a tree. The second and third are.

Proposition 21.3. *Let $G = (V, E, f)$ be a simple connected graph. The following conditions are equivalent*

(a) The graph G is a tree.
(b) For every two vertices $u, v \in V$, there is a unique simple path joining u, v.
(c) Removing any edge from the graph without removing any vertices creates a disconnected graph.

Proof. We will prove that (a) implies (b), that (b) implies (c) and that (c) implies (a). Then, by the transitivity of implications, we will have the equivalence of the three conditions. Let us start with

$(a) \Rightarrow (b)$. We assume that the graph is connected. Therefore, given two vertices, there is a path between the two. We proved in Proposition 19.3 (a), that if there is a path between two vertices, then there is also a simple path. Let us show that if G is a tree, the path is unique. Assume that there were two different paths from u to v

$$P = (u = v_0, e_1, v_1, \ldots, e_n, v_n = v), \quad P' = (u = v'_0, e'_1, v'_1, \ldots, e'_n, v'_{n'} = v)$$

Let us say that $e_1 = e'_1, \ldots, e_{i-1} = e'_{i-1}, e_i \neq e'_i$. Define the set

$$A = \{(j, j')|, j > i, j' > i, v_j = v'_{j'}\}$$

As $v_n = v'_{n'}$, $(n, n') \in A$ and therefore A is non-empty. Choose $(j, j') \in A$ with j the smallest possible. We now glue the path P between v_{i-1} and v_j with the path P' traveling backwards from $v_j = v'_{j'}$ to v_{i-1}

$$P'' = (v_{i-1}, e_i, v_i, \ldots, , v_{j-1}, e_j, v_j = v'_{j'}, e'_{j'}, v'_{j'-1}, \ldots, , e'_i, v'_{i-1} = v_{i-1})$$

This is a simple path, contradicting that G is a tree.

$(b) \Rightarrow (c)$ Let x be an edge of the graph, u, v the two vertices of x. If there is a simple path P in $G - \{e\}$ joining u, v, then there are two paths in G joining u, v, the path P and the path (u, x, v) contradicting the assumption in (b). Therefore, there is no simple path in $G - \{e\}$ joining u, v and from Proposition 19.3 (a), there is no path at all in $G - \{e\}$ joining u, v . Therefore, $G - \{e\}$ is disconnected.

$(c) \Rightarrow (a)$. Assume that removing any edge from the graph without removing any vertices creates a disconnected graph. Then, G cannot contain any cycles, as removing any edge from a cycle preserves connectedness. Hence, G is a tree. □

Part c of this proposition gives a simple way to check that a graph is a tree.

Example 21.4. The left graph in Figure 31 is not a tree as removing either of the edges $e_{5,7}, e_{5,8}, e_{7,8}$ the graph remains connected. The other two graphs are trees as removing any edge without removing vertices makes them disconnected.

Definition 21.5. Let $G = (V, E, f)$ be a simple connected graph. Then $v \in V$ is called **a leaf** if it has degree one.

Example 21.6. In the central graph in Figure 31 the vertices $v_1, v_4, v_7, v_8, v_9, v_{10}$ are leaves.

In the right graph in Figure 31 the vertices v_2, v_3, v_4, v_5 are leaves.

Proposition 21.7. *Let $G = (V, E, f)$ be a tree.*

(a) If G has at least two vertices, then G has at least two leaves.

(b) If $v \in V$ is a leaf of G, then removing from G the vertex v and the edge that has it as vertex, we obtain another tree.

Proof. (a) Let G be a tree with at least two vertices. Choose a maximal simple path in G

$$P = (v_0, e_1, v_1, \dots, e_n, v_n)$$

As G has at least two vertices and is connected, this path contains at least one edge and in particular, $v_0 \neq v_n$. We claim that v_0, v_n are leaves. Assume that v_0 were not a leaf. Then, there exists an edge e in addition to e_1 that has v_0 as vertex. If v' is its second vertex, we can form the path

$$\bar{P} = (v', e, v_0, e_1, v_1, \dots, e_n, v_n)$$

If the path $\bar{P}$ were not simple, this would mean that the edge e already appears in P. But this is not possible as then we would have a non-trivial closed path in G, contradicting that it is a tree. The existence of $\bar{P}$ as a simple path contradicts that P is maximal. Hence, v_0 has degree one.

Similarly, v_n has degree one and therefore G has at least two leaves.

(b) Let $v \in V$ be a leaf of G and G' the graph obtained by removing from G the vertex v and the edge that has it as vertex. As G had no cycles and G' is a subgraph of G, G' has no cycles. If we can prove that G' is connected, we will have shown that it is a tree. Take two vertices in G'. As G' is a subgraph of G, which is connected, there is a path joining the two vertices in G. If e is not one of the edges in the path, it is a path in G' and we are done. If e is one of the edges of the path, as v has degree one, the path begins or ends at v. But the path was meant to join two vertices in G' and v is not in G' contradicting our choice.

□

Proposition 21.7 allows to prove many results about trees by induction.

Proposition 21.8. *A tree with n vertices has $n-1$ edges*

Proof. We prove the result by induction on the number n of vertices.

Any simple graph wit one vertex has no edges. One single vertex with no edges is a tree. So, the result is correct for $n = 1$.

Assume the result is correct for any tree with at most n vertices. Consider a tree T with $n+1$ vertices. Write k for the number of edges of T. We know that T has a leaf v and that removing v and the edge x which has one vertex v, we obtain another tree T'. The tree T' has one fewer edge $k-1$ and one fewer vertex n that the tree T. Applying the induction assumption, $k-1 = n-1$. Hence, $k = n = (n+1)-1$, showing that the number of edges of T is one fewer than the number of vertices of T. □

Example 21.9. In the central graph in Figure 31 there are ten vertices and 9 edges.

In the right graph in Figure 31 there are six vertices and five edges.

Proposition 21.10. *Given a connected graph G, with n vertices and k edges, one can remove from G, $k-n+1$ edges to obtain a tree with still all n vertices.*

Proof. If G does not have any circuits, then it is a tree and $T = G$. Then $k = n-1$ and we need to remove 0 edges as claimed.

If G has a circuit, removing an edge from the circuit, the graph stays connected. Repeat the process so long as there is some circuit left. When no circuit is left, we have a tree where the number of edges is one less than the number of vertices. As no vertices have been removed, the number of vertices is still n and the new number of edges edges is $n-1$. Therefore, the number of edges to be removed is $k-n+1$. □

Example 21.11. The left graph in Figure 31 has $n = 10$ vertices and $k = 10$ edges. Note that $k - n + 1 = 1$. Removing either one of the edges e_1, e_2, e_3, we obtain a tree with $n = 10$ vertices and 9 edges.

22. Planar Graphs, December 6

We are interested in graphs that can be embedded in the plane without edges crossing. We will see that this is not possible for most graphs

Definition 22.1. A graph is said to be planar if it is isomorphic to a graph that can be embedded in the plane without the edges crossing

Example 22.2. (a) We usually sketch the complete simple graph K_4 on 4 vertices as shown in the left panel of Figure 32. We could have sketched it as in the second panel, so K_4 is planar.

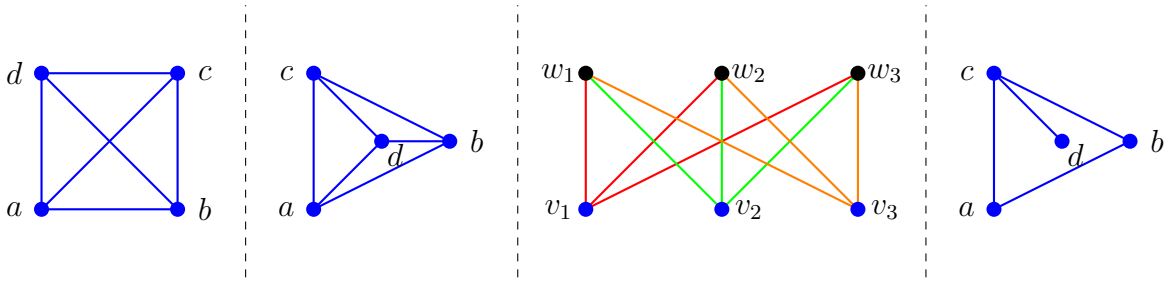


Figure 32. The first, second and fourth graphs are planar, as the first and second are isomorphic.The graph $K_{3,3}$ is not.

(b) A long time ago before the internet and video games, a popular entertainment for children used to be to try to solve the puzzle of three houses and three utilities. One should try to connect three houses to three different utilities so that the wires and tubes did not cross. A mathematical formulation of the problem is to find an embedding of $K_{3,3}$ as a planar graph. This could indeed keep kids busy for many hours, as we will see that no such solution exists.

A planar graph divides the plane into disjoint areas

Definition 22.3. Let$F$ be a planar graph. Each of the regions in which the graph divides the plane is called a **face**.

Example 22.4. The second graph in Figure 32 divides the plane into 4 faces. The fourth graph in Figure 32 divides the plane into 2 faces.

We want to show that $K_{3,3}$ is not planar. We will use implicitly the Jordan Curve Theorem.

Theorem 22.5. *[JordanCurve Theorem] A simple n-circuit embedded in the plane as a planar graph divides the plane into two regions, the bounded one inside and the unbounded one outside.*

This result seems simple but it is not easy to prove and we will not prove it here.

Proposition 22.6. *The graph $K_{3,3}$ is not planar.*

Proof. We will be using the Jordan Curve Theorem stating that a circuit sketched as a planar graph divides the plane into two regions, one inside and the other outside. Recall that the

graph $K_{3,3}$ has 6 vertices, $v_1, v_2, v_3, W_1, w_2, w_3$ with an edge joining every v_i to every w_j. Let us assume that we can draw this graph in the plane. Then

$$P = (v_1, e_{v_1w_1}, w_1, e_{v_2,w_1}, v_2, e_{v_2,w_2}, w_2, e_{v_1,w_2}, v_1)$$

is a 4 circuit and therefore divides the plane into two regions

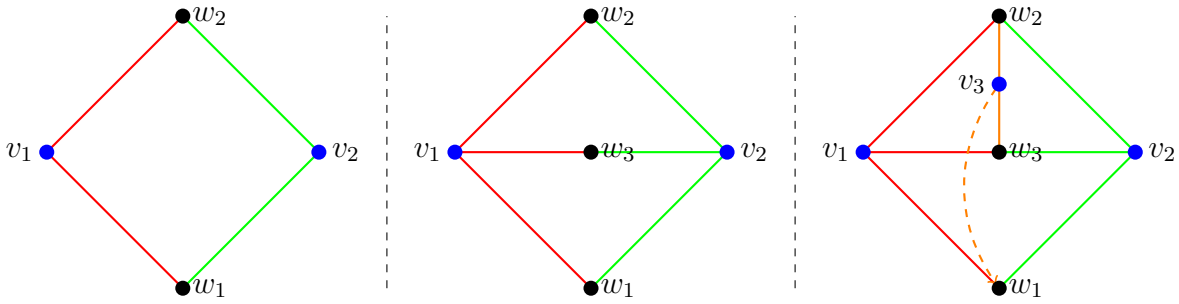


FIGURE 33. The graph $K_{3,3}$ is not planar.

The vertex w_3 is in one of these regions and the edges $e_{v_1w_3}, e_{v_2,w_3}$ divide that region into two, so that we now have 3 regions with respective boundaries

$$P_{2,3} = (v_1, e_{v_1w_3}, w_3, e_{v_2,w_3}, v_2, e_{v_2,w_2}, w_2, e_{v_1w_2}, v_1),\ P_{1,3} = (v_1, e_{v_1w_1}, w_1, e_{v_2,w_1}, v_2, e_{v_2,w_3}, w_3, e_{v_1w_3}, v_1),$$

$$P_{1,2} = (v_1, e_{v_1w_2}, w_2, e_{v_2,w_2}, v_2, e_{v_2,w_1}, w_1, e_{v_1w_1}, v_1)$$

The remaining vertex v_3 is in only one of these regions. Only two of the vertices w_i are in the boundary of each region. For example, if v_3 is in the region bounded by $P_{2,3}$, then v_3 can be joined to w_2, w_3 with the graph remaining planar but not to w_1 as a potential edge $e_{v_3w_1}$ will intersect one of the four edges $e_{v_1w_3}, e_{v_2,w_3}, e_{v_2,w_2}, e_{v_1w_2}$ in the boundary of the region. □

Definition 22.7. Let F be a planar graph. We define the Euler characteristic (also called Euler number or Euler-Poncaré characteristtic) of the graph $\chi(G) == |V| - |E| + |F|$.

The Euler-Poincaré characteristic can be defined for more general objects than a planar graph. The definition , as is, would work for any graph contained in some surface. Notice that we take alternative sum of the objects starting with the smallest (vertices) and ending with the biggest (faces). A generalization of this definition would apply to polyhedra in three space for which $\chi(G) = |V| - |E| + |F| - |R|$ where R is the number of three dimensional regions in which the space is divided and with a similar definition to higher dimensional objects. The Euler-Poincaré characteristic is that it is an invariant of the space in which the object lives. It measures topological properties of the objects, that is properties that would not change if you were to stretch the objects without breaking them. The first result in this direction is the following Theorem:

Theorem 22.8. *[Euler's Formula] Given a connected planar graph, let F be the set of faces in which it divides the plane. Then, we have the equation*

$$\chi(G) = |V| - |E| + |F| = 2$$

Proof. We can prove this by induction on the number of edges.

The base case of the induction is $|E| = 0$. Such a connected graph will have only one vertex and will not separate the plane. Hence

$$|V| = 1,\ |E| = 0,\ |F| = 1;\quad |V| - |E| + |F| = 1 - 0 + 1 = 2$$

as claimed.

Assume the result is correct for any connected graph with n edges and prove it for a connected graph with $n + 1$ edges. We first want to check that we can remove from a connected graph (with at least one edge of course) a suitable chosen edge and the end vertex in the case the chosen edge is a leaf and obtain a graph that is still connected: if the graph is a tree, it has a leaf and we already checked that removing a leaf together with the end vertex from a connected graph, the graph stays connected. If the graph has no leaves, then, it contains a circuit. Removing an edge from a simple circuit also keeps the graph connected.

Note also that removing an edge from a planar graph keeps the graph planar, as there are fewer edges there will be fewer but certainly not more, edge crossings.

Assume first that we go from the planar graph G with $|V|$ vertices, $|E|$ edges and $|F|$ faces to a graph G' by removing a leaf. The new graph G' will have $|V'| = |V| - 1$ vertices, $|E'| = |E| - 1$ edges. The number of faces will stay the same, as a leaf cannot create a division of a face, that is $|F'| = |F|$. Therefore

$$\chi(G) = |V| - |E| + |F| = |V'| + 1 - (|E'| + 1) + |F'| = |V'| - |E'| + |F'| = \chi(G')$$

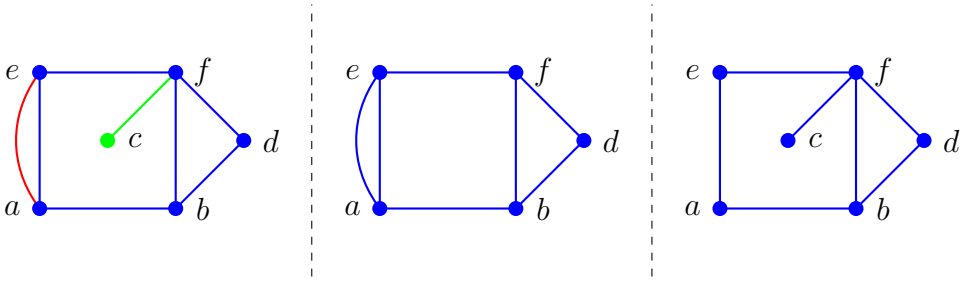


FIGURE 34. Removing a leaf (green) or an edge that is part of a circuit (red) to obtain another planar graph.

Assume then that we go from the planar graph G with $|V|$ vertices, $|E|$ edges and $|F|$ faces to a graph G' by removing an edge that is part of a circuit. The new graph G' will have $|V'| = |V|$ vertices, $|E'| = |E| - 1$ edges. The number of faces will decrease in one as one can now move from the region inside the circuit to the region outside by moving across what used to be the edge. Therefore

$$\chi(G) = |V| - |E| + |F| = |V'| - (|E'| + 1) + (|F'| + 1) = |V'| - |E'| + |F'| = \chi(G')$$

So, in both cases, the graph with $n+1$ edges satisfies that $\chi(G) = \chi(G')$. From the induction assumption, $\chi(G') = 2$. Therefore, $\chi(G) = 2$ as claimed. □

Example 22.9. (a) The graph K_4 is planar as shown in the second picture of Figure 32. It has 4 vertices, 6 edges and 4 faces. So, $|V| - |E| + |F| = 4 - 6 + 4 = 2$.

(b) The left graph in Figure 22 has 6 vertices, 8 edges and 4 faces. So, $|V| - |E| + |F| = 6 - 8 + 4 = 2$.

The middle graph in this Figure has one fewer edge and one fewer region but the same number of vertices, as we removed an edge in a cycle.

The middle graph in this Figure has one fewer edge and one fewer vertex but the same number of faces, as we removed a leaf.

Definition 22.10. The **degree** of a face is the number of edges that delimit this face where an edge that sticks inside a single face is counted twice towards the degree of that face.

Proposition 22.11. *The sum of the degrees of the faces of a planar graph is twice the number of edges.*

Proof. Every edge contributes to the degree of the two faces that it limits with. □

Example 22.12. The left graph in Figure 22 divides the plane into 4 faces, one between the two multiedges with vertices a, e that has degree 2. The square face in the center has degree 6. The triangular left to the side has degree 3. The unbounded face has degree five.

We will now use Euler's formula to prove an inequality between the number of vertices and edges of a planar graph.

Proposition 22.13. *(a) Every simple planar graph with at least 3 vertices satisfies*

$$|E| \leq 3|V| - 6$$

(b) Every simple planar graph with at least 3 vertices and no 3-cycles satisfies

$$|E| \leq 2|V| - 4$$

Proof. (a) A simple planar graph with 3 vertices has at most 3 edges, so the result is true in this case.

In a simple planar graph, the degree of any face is at least three. Moreover, we know from 22.11 that the sum of the degrees of the faces is twice the number of edges. Then

$$3|F| \leq \sum \deg(f_i) = 2|E|$$

We can assume the graph is connected, otherwise we could add edges joining the different connected components. Then we can use Euler's formula $|V| - |E| + |F| = 2$ and substituting the inequality for the face inn term of edges

$$2 = |V| - |E| + |F| \leq |V| - |E| + \frac{2}{3}|E| = |V| - \frac{1}{3}|E|$$

This can be rewritten as

$$|E| \leq 3|V| - 6$$

which is the desired inequality.

(b) If the graph does not contain triangles, then every face has degree at least 4. Therefore, the inequality we have this time around is

$$4|F| \leq \sum \deg(f_i) = 2|E|$$

Then,

$$2 = |V| - |E| + |F| \leq |V| - |E| + \frac{2}{4}|E| = |V| - \frac{1}{2}|E|$$

which can be rewritten as

$$|E| \leq 2|V| - 4$$

□

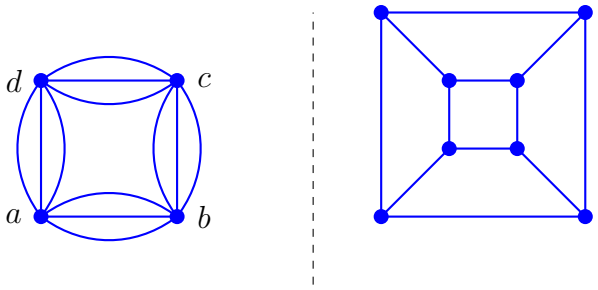


FIGURE 35. The left graph is not simple and does not satisfy the bounds. In the right graph, the inequality for graphs not containing triangles is an equality

Example 22.14. (a) The result is false if the graph is not simple because a multi-edge can create a face of degree 2. For example, the left graph in Figure 35 has 4 vertices and 12 edges and $12 > 3 \times 4 - 6$.

(b) These inequalities cannot be improved if the graph contains triangles or if the graph does not contain triangles but contains squares respectively. For example, in the right graph of Figure 35, the graph does not contain triangles. It has 8 vertices and 12 edges and $12 = 2 \times 8 - 4$.

Corollary 22.15. *(a) The complete graph on 5 vertices K_5 in non-planar.*
(b) The complete bipartite graph $K_{3,3}$ is non-planar

Proof. (a) The graph K_5 has five vertices and $\binom{5}{2} = 10$ edges. As, $10 > 9 = 3 \times 5 - 6$, from Proposition 22.13, K_5 is not planar.

(b) No bipartite graph contains triangles: given three vertices, at least two of them belong to the same set of the partition and therefore there cannot be an edge between them.

Note that $K_{3,3}$ contains 6 vertices and 9 edges. As, $9 > 8 = 2 \times 6 - 4$, from Proposition 22.13 (b), $K_{3,3}$ is not planar.

□

While $K_{3,3}$ is not a planar graph, it can be immersed in the surface of a donut. The surface of a donut can be obtained by taking a rectangular flat piece of paper, or better a slightly stretchy material and gluing parallel edges. We show below how to sketch $K_{3,3}$ on the rectangle when we identify the edges to form a torus:

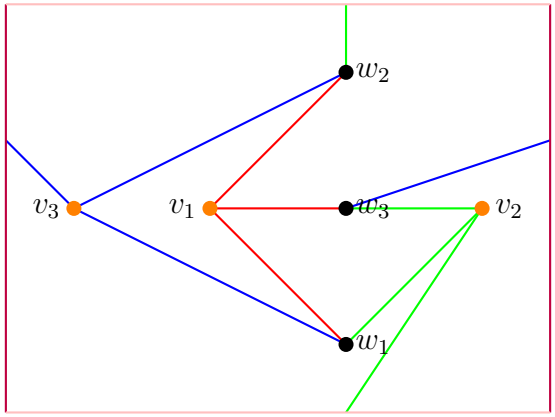


FIGURE 36. The graph $K_{3,3}$ in the torus.

23. The four color problem and graph coloring, December 8.

A famous mathematical question is the four color problem: given a map of countries, we want to color it with the smallest number possible of colors so that each country is painted in a single color and countries that share a border have different colors. In the nineteenth century, it was suggested that four colors should be enough. It took close to a hundred years to show that this is correct. This is an interesting math question that you can explain to a five year old. Part of the fame of the problem comes from the way it was solved. It was the first time in the history of Mathematics in which a portion of the proof was delegated to a computer program. The program reduced the number of cases to be examined to a manageable number.

We first translate the question to graph theory: Given a map of countries, we are going to assume that each country is in one piece. Place a vertex inside each country. Join two of these vertices if the countries share a border. We want to color the vertices so that adjacent vertices are painted in different colors. Equivalently, we want a function from the set of vertices to the set of colors so that the inverse image of a color is an independent set. So, we can think of trying to write the vertices of a graph as a disjoint union of the smallest possible number of independent sets.

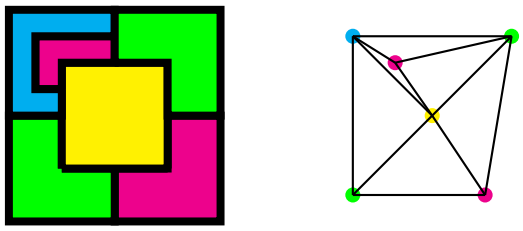


Figure 37. The graph corresponding to a country configuration

In the case of starting with the map of a country, the graph that we obtain is a planar graph. It is not true that for arbitrary graphs, the smallest number of colors is 4. Let us define this properly:

Definition 23.1. Given a graph $G = (V, E, f)$, **a coloring** of the graph is a function $g : V \to C$, where C is called the set of colors such that the images of adjacent vertices are different.

The chromatic number $CN(G)$ is the smallest number of elements of a set C such that there exists a coloring function $g : V \to C$.

Then the four color Theorem can be stated as follows

Theorem 23.2. *[Four color Theorem] The chromatic number of a planar graph is four.*

Let us look at small chromatic numbers:

Proposition 23.3. *(a) The chromatic number of a graph is one if and only if $E = \emptyset$*
(b) The chromatic number of a graph is two if an only if the graph is bipartite and has at least one edge.

Proof. (a) Recall that a coloring function must have different images for adjacent vertices. If the chromatic number of a graph is one, then no two vertices are adjacent which is the same as saying that $E = \emptyset$.

(b) By definition, a graph is bipartite if the vertices can be written as the union of two disjoint sets, so that there are no edges among the elements of a single set. If the graph is bipartite, we can color the vertices of one set with one color and the vertices of the other set with the second color. Conversely, if the chromatic number of a graph is two, we can take as the vertices of each set of the partition the inverse image of one of the coloring elements.

□

Example 23.4. (a) The chromatic number of a cycle C_n is 2 if n is even, it is 3 if n is odd: If n is even, choose alternating colors for the vertices.

If n is odd, vertices with even and odd indices must have different colors. But the first and last must have different colors. So, we need a third color for the last vertex.

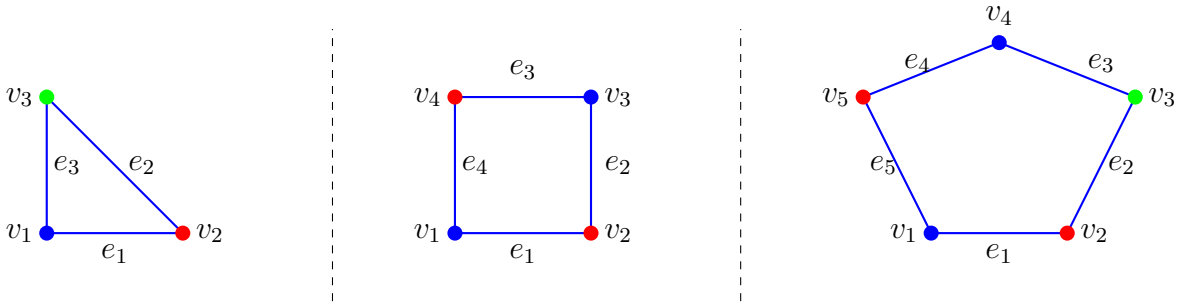


FIGURE 38. Coloring of cycles

(b) The chromatic number of K_n is n as each vertex is adjacent to every other vertex, so no two vertices can have the same color.

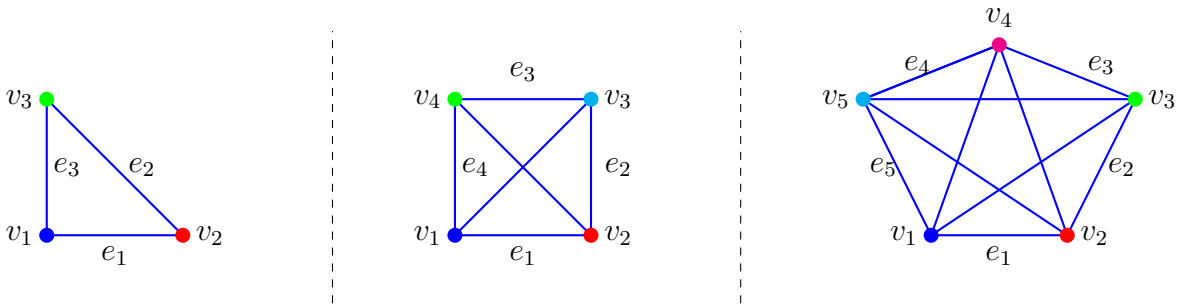


FIGURE 39. Coloring of complete graphs

The four color problem is very difficult to prove, the six color is easy:

Proposition 23.5. *(a) Any simple planar graph has a vertex of degree at most 5.*
(b) Any simple planar graph has chromatic number at most six.

Proof. (1) Assume that $G = (V, E, f)$ is planar and that all its vertices have degree at least 6. Then by the handshake lemma

$$2|E| = \sum_{v \in V} \deg(v) \geq \sum_{v \in V} 6 = 6|V| \Longrightarrow |E| \geq 3|V|.$$

But we know $|E| \leq 3|V| - 6$ since G is planar, so we have a contradiction.

(2) Proceed by induction on the number of vertices of the graph.

For the base case, a graph with 1 vertex only requires one color and $1 \leq 6$, so the result is correct in this case.

Assume now that any simple planar graph with at most $n-1$ vertices is 6 colorable and let G be a simple planar graph with n vertices. Let v be a vertex of degree less than 6 (which exists by part (a)). Delete v and its incident edges from G get get a graph G' with $n-1$ vertices. As G' is still planar and simple, it is 6 colorable by the induction hypothesis. We can now obtain G by adding v back to G' with the at most 5 edges that were deleted with v. Since v is connected to at most 5 vertices, we can pick the 6th color for v. Thus the 6-coloring on G' gives us a 6-coloring on G, as needed.

□

24. Limits of sequences, Cauchy sequences, Dec 8

Remember that a sequence of numbers (integers, rational, real, complex...) is a collection of numbers indexed by the natural numbers $(a_n)_{n\in\mathbb{N}}$. We played with sequences when we were talking about recursion, we were then using an inductive process to define a sequence. Sequences play an important role in the study of Calculus. In fact, a certain type of sequences, called Cauchy sequences can be used to define real numbers. We will see this next week. A more formal definition of sequence would be

Definition 24.1. A sequence of rational numbers is a function $\mathbb{N} \to \mathbb{Q}$

A sequence of real numbers is a function $\mathbb{N} \to \mathbb{R}$

You are familiar from Calculus with the concept of convergence of sequences, although you probably did not define it formally. The intuitive idea of a sequence with limit L is that the values of a_n come as close as L as we want. Being "as close as we want" means that it is at a distance smaller than any fixed positive amount we may want to fix. As distance in the number line is measured by the absolute value, we can formalize this as follows:

Definition 24.2. A sequence a_n of rational numbers is said to converge to $L \in \mathbb{Q}$ if for any $\epsilon \in \mathbb{Q}, \epsilon > 0$, there exists some $m \in \mathbb{N}$ such that for all $n \geq m$, $|a_n - L| < \epsilon$.

Similarly, a sequence a_n of real numbers is said to converge to $L \in \mathbb{R}$ if for any $\epsilon \in \mathbb{Q}, \epsilon > 0$ there exists some $m \in \mathbb{N}$ such that for all $n \geq m$, $|a_n - L| < \epsilon$.

When the sequence (a_n) converges to a value L, we write $\lim_{n\to\infty} a_n = L$

The definition just says that starting with a_m, all the terms of the sequence are at distance less than any number we want from L. We think of ϵ as a small number. Note that this m should be a function of ϵ.

Example 24.3. (a) The sequence

$$a_0 = 1, a_1 = -1, a_2 = 1, a_3 = -1, \ldots, a_n = (-1)^n$$

does not convergence. Let us prove this formally: If $l \neq 1$, then $|l - 1| = b > 0$. Choose $\epsilon = \frac{b}{2} < b$. For the even values of n,

$$|a_n - l| = |1 - l| = b > \frac{b}{2} = \epsilon$$

This means that the limit cannot be $l \neq 1$. It cannot be $l = 1$ either because the a_n for n odd are at distance 2 of $l = 1$ and therefore the distance cannot be made less than ϵ for any $\epsilon < 2$.

(b) The sequence $a_n = \frac{n+3}{n+2} \in \mathbb{Q}$ has limit 1: Let us compute the difference between a_n and 1.

$$|a_n - 1| = \left|\frac{n+3}{n+2} - 1\right| = \left|\frac{n+3-(n+2)}{n+2}\right| = \frac{1}{n+2}$$

Given $\epsilon \in \mathbb{Q}, \epsilon > 0$, take $m \geq \frac{1}{\epsilon} - 2$. Then,

$$\forall n \geq m, \quad |a_n - 1| = \frac{1}{n+2} \leq \frac{1}{m+2} = \epsilon.$$

(c) The sequence of rational numbers

$$a_0 = 0, a_1 = 0.3, a_2 = 0.33, a_3 = 0.333, a_4 = 0.3333, a_5 = 0.3333, a_6 = 0.333333, \ldots$$

and in general a_n has zero for the integral part, the first n digits after the decimal point being threes and zeroes afterwards. The limit of this sequence is $\frac{1}{3} \in \mathbb{Q}$: $\frac{1}{3} - a_n$ has zero integral part and the first n digits equal to zero. Therefore, $|a_n - \frac{1}{3}| < \frac{1}{10^n}$. Then $|a_n - \frac{1}{3}| < \epsilon$ if $\frac{1}{10^n} < \epsilon$ or equivalently $n \geq \frac{-\ln \epsilon}{\ln 10}$.

(d) The sequence of rational numbers

$$a_0 = 3, a_1 = 3.1, a_2 = 3.14, a_3 = 3.141, a_4 = 3.1415, a_5 = 3.14159, a_6 = 3.141592, \ldots$$

and in general a_n has the first n digits of the decimal expansion of π and zeros afterwards. The limit of this sequence does not exist in $\mathbb{Q}$. Assume the limit L did exist. For each j, choose $\epsilon = \frac{1}{10^{j+1}}$. then there exists some m such that for all $n \geq m$ $|a_n - L| \leq \frac{1}{10^{j+1}}$. It follows that the first j digits of L agree with the first j digits of π. This would be true for every j. Therefore, $L = \pi \notin \mathbb{Q}$.

The limit of a sequence does not necessarily exist, but if it does, it is unique. Also, limits are compatible with addition and products.

Proposition 24.4. *Consider a sequence of rational or real numbers (a_n).*

(a) The limit if it exists is unique: If $\lim_{n\to\infty} a_n = L$, $\lim_{n\to\infty} a_n = L'$, then $L = L'$.

(b) Any constant sequence $a_n = a$, $\forall n$ converges to $L = a$.

(c) Multiplication with scalars is compatible with limits: If $\lim_{n\to\infty} a_n = L, c \in \mathbb{Q}$, then $\lim_{n\to\infty}(ca_n) = cL$.

(d) Addition of sequences is compatible with limits: If $\lim_{n\to\infty} a_n = L$, $\lim_{n\to\infty} a'_n = L'$, then $\lim_{n\to\infty}(a_n + a'_n) = L + L'$.

(e) Product of sequences is compatible with limits: If $\lim_{n\to\infty} a_n = L$, $\lim_{n\to\infty} a'_n = L'$, then $\lim_{n\to\infty}(a_n a'_n) = LL'$.

Proof. (a) Assume that $\lim_{n\to\infty} a_n = L$, $\lim_{n\to\infty} a_n = L'$. If $L \neq L'$, then $|L - L'| = b > 0$. Choose $\epsilon < \frac{b}{2}, \epsilon > 0$. There exist $m, m' \in \mathbb{N}$ such that if $n \geq m$, then $|a_n - L| < \epsilon$, if $n \geq m'$, then $|a_n - L'| < \epsilon$. Take $n \geq \max\{m, m'\}$, then

$$b = |L - L'| = |(L - a_n) + (a_n - L')| \leq |L - a_n| + |a_n - L'| \leq 2\epsilon < b$$

which is a contradiction.

(b) Any constant sequence $a_n = a$ $\forall n$ satisfies $|a_n - L| = |a - a| = 0 < q$ for any positive $q \in \mathbb{Q}$. Therefore, it converges to $L = a$ by definition of limit.

(c) Assume that $\lim_{n\to\infty} a_n = L$ and let c be a rational number. Choose $\epsilon \in \mathbb{Q}^+$. From the convergence of the sequence, there exist $m \in \mathbb{N}$ such that if $n \geq m$, then $|a_n - L| < \frac{\epsilon}{|c)}$, if $n \geq m'$. Then also

$$|ca_n - cL| = |c||(a_n - L| \leq |c|\frac{\epsilon}{|c)} = \epsilon$$

showing that $\lim_{n\to\infty}(ca_n) = cL$.

(d) Assume that $\lim_{n\to\infty} a_n = L$, $\lim_{n\to\infty} a'_n = L'$. Choose $\epsilon \in \mathbb{Q}^+$. Then $\frac{\epsilon}{2} \in \mathbb{Q}^+$. From the convergence of the sequences, there exist $m, m' \in \mathbb{N}$ such that if $n \geq m$, then $|a_n - L| < \frac{\epsilon}{2}$, if $n \geq m'$, then $|a'_n - L'| < \frac{\epsilon}{2}$. Take $n \geq \max\{m, m'\}$, then

$$|(a_n + a'_n) - (L + L')| = |(a_n - L) + (a'_n - L')| \leq |a_n - L| + |a'_n - L'| \leq \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$$

showing that $\lim_{n\to\infty}(a_n + a'_n) = L + L'$.

(e) Assume that $\lim_{n\to\infty} a_n = L$, $\lim_{n\to\infty} a'_n = L'$. Choose $\epsilon \in \mathbb{Q}^+$. From the convergence of the sequences, there exist $m, m' \in \mathbb{N}$ such that if $n \geq m$, then $|a_n - L| < \frac{\epsilon}{2(|L'|+1)}$, if $n \geq m'$, then $|a'_n - L'| < \frac{\epsilon}{2(|L|+1)}, |a'_n - L'| < 1$ Then also

$$|a'_n| = |(a'_n - L') + L| \leq |a'_n - L'| + |L'| \ < 1 + |L'|.$$

Take $n \geq \max\{m, m'\}$, then

$$|(a_n a'_n) - (LL')| = |(a_n - L)a'_n + L(a'_n - L')| \leq |a_n - L||a'_n| + |L||a'_n - L'| \leq$$
$$\leq \frac{\epsilon}{2(|L'|+1)}(|L'|+1) + \frac{\epsilon}{2(|L|+1)}|L| < \epsilon$$

showing that $\lim_{n\to\infty}(a_n.a'_n) = LL'$.

□

We now want to introduce Cauchy sequences. These are sequences that do not necessarily converge (in $\mathbb{Q}$), but in which the terms come very close to each other. In a way, Cauchy sequences are sequences that "should" converge, except that there may be a hole in the rational line where the limit should be. Real numbers are constructed to fill these holes and they come up as equivalence classes of Cauchy sequences of rational numbers.

Definition 24.5. A sequence (a_n) of rational numbers is said to be a Cauchy sequence if for any $\epsilon \in \mathbb{Q}, \epsilon > 0$, there exists some $m \in \mathbb{N}$ such that for all $n_1, n_2 \geq m$, $|a_{n_1} - a_{n_2}| < \epsilon$.

Proposition 24.6. *Consider a sequence of rational or real numbers (a_n).*
(a) If (a_n) converges, then (a_n) is a Cauchy sequence.
(b) If $(a_n), (a'_n)$ are Cauchy sequences, then $(a_n + a'_n)$ is a Cauchy sequence.
(c) If (a_n) is a Cauchy sequence, then its terms are bounded: there exists $A > 0$ such that $|a_n| < A$ for all $n \in \mathbb{N}$.
(d) If $(a_n), (a'_n)$ are Cauchy sequences, then $(a_n a'_n)$ is a Cauchy sequence.

Proof. (a) Assume that $\lim_{n\to\infty} a_n = L$. If $L \neq L'$, then $|L - L'| = b > 0$. Choose $\epsilon \in \mathbb{Q}$. From the convergence of the sequences, there exist $m \in \mathbb{N}$ such that if $n \geq m$, then $|a_n - L| < \frac{\epsilon}{2}$. Take $n_1, n_2 \geq m$, then

$$|a_{n_1} - a_{n_2}| = |a_{n_1} - L + L - a_{n_2}| \leq |a_{n_1} - L| + |L - a_{n_2}| \leq \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$$

proving that (a_n) is a Cauchy sequence.

(b) Assume that $(a_n), (a'_n)$ are Cauchy sequences. Choose $\epsilon \in \mathbb{Q}, \epsilon > 0$, there exists then some $m, m' \in \mathbb{N}$ such that for all $n_1, n_2 \geq m$, $|a_{n_1} - a_{n_2}| < \frac{\epsilon}{2}$ and for all $n_1, n_2 \geq m'$, $|a'_{n_1} - a'_{n_2}| < \frac{\epsilon}{2}$. Let $n_1, n_2 \geq \max\{m, m'\}$. Then,

$$|(a_{n_1} + a'_{n_1}) - (a_{n_2} + a'_{n_2}) = |(a_{n_1} - a_{n_2}) + (a'_{n_1} - a'_{n_2})| \leq \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$$

proving that $a_n + a'_n$ is a Cauchy sequence.

(c) Assume that (a_n) is a Cauchy sequence There exists then some $m' \in \mathbb{N}$ such that for all $n_1, n_2 \geq m$, $|a_{n_1} - a_{n_2}| < 1$. In particular, for any $n \geq m_1$,

$$|a_n| = |(a_n - a_m) + a_m| \leq |a_n - a_m| + |a_m| \leq 1 + |a_m|$$

Take $A = \max\{|a_0|, |a_1|, \ldots, |a_{m-1}|, 1 + |a_m|\}$. We just proved that any $|a_n|, n \geq m$ is bounded by A, while the first m terms are also bounded by A by definition of A.

(d) Assume that $(a_n), (a'_n)$ are Cauchy sequences. There exists bounds, $A > 0, A' > 0$ such that $|a_n| < A, |a'_n| < A'$ for all $n \in \mathbb{N}$.

Choose $\epsilon \in \mathbb{Q}, \epsilon > 0$, There exists then some m such that for all $n_1, n_2 \geq m$, $|a_{n_1} - a_{n_2}| < \frac{\epsilon}{2A'}$, $|a'_{n_1} - a'_{n_2}| < \frac{\epsilon}{2A}$. Let $n_1, n_2 \geq m$. Then,

$$|(a_{n_1}a'_{n_1}) - (a_{n_2}a'_{n_2}) = |(a_{n_1} - a_{n_2})a'_{n_1} + a_{n_2}(a'_{n_1} - a'_{n_2})| \leq |a_{n_1} - a_{n_2}||a'_{n_1}| + |a_{n_2}||a'_{n_1} - a'_{n_2}| \leq$$

$$\leq \frac{\epsilon}{2A'}A' + \frac{\epsilon}{2A}A = \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$$

proving that $a_n a'_n$ is a Cauchy sequence.

□

25. The real numbers, Dec 13

We saw in a homework question how to construct the integers starting with the natural numbers: Take A the set of pairs of natural numbers and define a relation in A by

$$(a,b),(c,d) \in A, \quad (a,b) \sim (c,d) \text{ if and only if } a+d=b+c.$$

There is a bijection between the set of equivalence classes and the set of integers. Addition in the set of integers comes from addition component-wise in the set of pairs while multiplication must be defined by

$$[(a,b)][(c,d)] = [(ac+bd, ad+bc)].$$

Both operations are well defined, meaning that they are compatible with the equivalence relation.

Similarly, we saw how to construct the rational numbers from the integers as follows: In the set of pairs of integers, the second one not being zero $A = \mathbb{Z}\times(\mathbb{Z}-\{0\})$ define a relation $\sim$ by $(a,b) \sim (c,d)$ if and only if $ad=bc$, the equivalence classes are rational numbers, usually written as $\frac{a}{b}$ rather than $[(a,b)]$ (the condition that $b \neq 0$ means that the fraction makes sense). The equivalence relation is equality of fractions. Product is defined component-wise while addition is given as

$$[(a,b)] + [(c,d)] = [(ad+bc, bd)]$$

Again, both operations are well defined, meaning that they are compatible with the equivalence relation.

We now want to construct the real numbers from the rational numbers by defining an equivalence relation on the set of Cauchy sequences of rational numbers:

Definition 25.1. Let A be the set of Cauchy sequences of rational number. For $(a_n), (a'_n) \in A$, we say that $(a_n) \sim (a'_n)$ if and only if $\lim_{n\to\infty}(a_n - a'_n) = 0$ where $(a_n - a'_n)$ is the sequence whose n^{th} term is the difference of the n^{th} terms of the two given sequences.

In symbols, this can be written as

$$(a_n) \sim (a'_n) \iff \forall \epsilon \in \mathbb{Q}^+, \exists m \in \mathbb{N} \text{ such that } \forall n \geq m,\ |a_n - a'_n| < \epsilon.$$

Lemma 25.2. *The relation defined in 25.1 is an equivalence relation.*

Proof. We need to show that the relation is reflexive, symmetric and transitive:

- Reflexive means that each sequence is equivalent to itself, that is, $\lim_{n\to\infty}(a_n - a_n) = 0$ This is satisfied as $a_n - a_n = 0$.
- Symmetric: assume that $(a_n) \sim (a'_n)$. Then $\lim_{n\to\infty}(a_n - a'_n) = 0$. From Proposition 24.4 (c), multiplication with scalars is compatible with limits. Therefore,

  $$\lim_{n\to\infty}(a'_n - a_n) = \lim_{n\to\infty}(-1)(a_n - a'_n) = (-1)\lim_{n\to\infty}(a_n - a'_n) = (-1)\times 0 = 0$$

  which means that $(a'_n) \sim (a_n)$.
- Transitive: assume that $(a_n) \sim (a'_n)$, $(a'_n) \sim (a"_n)$. Then $\lim_{n\to\infty}(a_n - a'_n) = 0$, $\lim_{n\to\infty}(a'_n - a"_n) = 0$. From Proposition 24.4 (d), addition of sequences is compatible with limits. Therefore,

$$\lim_{n\to\infty}(a_n - a"_n) = \lim_{n\to\infty}[(a_n - a'_n) + (a'_n - a"_n)] = \lim_{n\to\infty}(a_n - a'_n) + \lim_{n\to\infty}(a'_n - a"_n) = 0+0 = 0$$

  which means that $(a_n) \sim (a"_n)$.

□

Definition 25.3. The set of equivalence classes of Cauchy sequences by the equivalence relation define in Definition 25.1 is the set of real numbers.

If we want to have a set of numbers, we should be able to add subtract multiply and divide (so long as the divisor is not zero). We see next that addition and product are well defined

Proposition 25.4. *Given Cauchy sequences with* $(a_n) \sim (a'_n), (b_n) \sim (b'_n)$*, then*
(a) $(a_n + b_n) \sim (a'_n + b'_n)$
(b) $(a_n b_n) \sim (a'_n b'_n)$.

Proof. (a) Recall that from Proposition 24.6(b) if $(a_n), (b_n)$ are Cauchy sequences, then $(a_n + b_n)$ is a Cauchy sequence (and similarly $(a'_n + b'_n)$ is a Cauchy sequence). From the definition of equivalence, $\lim_{n\to\infty}(a_n - a'_n) = 0, \lim_{n\to\infty}(b_n - b'_n) = 0$. From Proposition 24.4 (b), the limit of the sum is sum of limits. Hence,

$$\lim_{n\to\infty}(a_n+b_n)-(a'_n+b'_n) = \lim_{n\to\infty}(a_n-a'_n)+(b_n-b'_n) = \lim_{n\to\infty}(a_n-a'_n)+\lim_{n\to\infty}(b_n-b'_n) = 0+0 = 0$$

proving that $(a_n + b_n) \sim (a'_n + b'_n)$.

(b) From Proposition 24.6(c), if $(a_n), (b_n)$ are Cauchy sequences, then there exists $A > 0, B > 0$ such that $|a_n| < A, |b_n| < B$ for all $n \in \mathbb{N}$. Choose $\epsilon \in \mathbb{Q}^+$. There exists m such that if $n \geq m$, then $|a_n - a'_n| \leq \frac{\epsilon}{2B}, |b_n - b'_n| \leq \frac{\epsilon}{2A}$ Then, for $n \geq m$,

$$|(a_n b_n) - (a'_n b'_n)| = |(a_n - a'_n)b_n + a'_n(b_n - b'_n)| \leq |a_n - a'_n||b_n| + |a'_n||b_n - b'_n|| \leq$$
$$\leq \frac{\epsilon}{2B}B + \frac{\epsilon}{2A}A = \epsilon$$

proving that $(a_n b_n) \sim (a'_n b'_n)$.

□

This allows us to define addition and product of real numbers as follows

Definition 25.5. Given Cauchy sequences $(a_n), (b_n)$, we define the sum and product of their cosets as follows

- $[(a_n)] + [(b_n)] = [(a_n + b_n)]$
- $[(a_n)][(b_n)] = [(a_n b_n)]$

These definitions make sense because, as we proved in 25.4, the coset of the sum does not depend on the representative of the coset we take and same thing with product.

These definitions allow us to prove all the usual properties of addition and product. like associativity and commutativity for addition and product and the distributive property of addition with respect to product. They follow from the definition of addition and product and from the same properties in the set of rational numbers. By thinking of a rational number as the constant Cauchy sequence with all terms equal to that number, we can immerse the rational numbers in the set of real numbers. We can also define an order in the real numbers, an absolute value and even what we mean by a Cauchy sequence of real numbers.

Before we do that though, we want to look at how to think of an equivalence class of Cauchy sequences as a number I am guessing that equivalence classes of Cauchy sequences does not look much like numbers to you .

Recall that rational numbers are defined (as we mentioned at the beginning of this section) as quotients of two integers. By dividing the two integers using long division, we come up

with a decimal expression. Let us review how rational numbers can be characterized by their decimal expression.

Proposition 25.6. *(a) Every rational number has a decimal expression that either terminates or repeats.*

(b) Given a decimal expression that either terminates or repeats, it corresponds to a rational number.

Proof. (a) A rational number is of the form $\frac{a}{b}$ where a, b are integers. We can obtain the decimal expression by long division. The successive remainders should be less than b, so there is a finite number of potential remainders. This means that at some point, they should start repeating (possibly with zeroes). Therefore, the decimal expression of a rational number either terminates or repeats.

(b) Assume given a decimal expression that either terminates or repeats. Let us see it comes from the quotient of two integers, and therefore corresponds to a rational number. If the expression terminates, we write a_i for the n^{th} digit of the integral part and a'_i for the n^{th} digit of the decimal expression. Then, the number is of the form

$$a_n a_{n-1} \dots a_1 a_0 \cdot a'_1 a'_2 \dots a'_k.$$

We can write this number as the quotient of two integers in the form

$$a_n a_{n-1} \dots a_1 a_0 \cdot a'_1 b_2 \dots a'_k = \frac{a_n a_{n-1} \dots a_1 a_0 a'_1 a'_2 \dots a'_k}{10^k}$$

If the expression repeats, with similar notations as in the previous case, the number is of the form $x = a_n a_{n-1} \dots a_1 a_0 \cdot a'_1 \dots a'_k b_1 b_2 \dots b_m b_1 b_2 \dots b_m b_1 b_2 \dots b_m \dots$. Then,

$$y = x - a_n a_{n-1} \dots a_1 a_0 \cdot a'_1 \dots a'_k. = \cdot 0 \dots 0 b_1 b_2 \dots b_m b_1 b_2 \dots b_m b_1 b_2 \dots b_m \dots.$$

Notice now that

$$(10^{m+k} - 1)y = 10^{m+k} y - y = b_1 b_2 \dots b_m$$

Therefore y is the quotient of two integers as we can write it in the form

$$y = \frac{b_1 b_2 \dots b_m}{10^{k+m} - 1}$$

Then $x = a_n a_{n-1} \dots a_1 a_0 \cdot a'_1 \dots a'_k + y$ is the sum of a terminating number, that we showed is rational and a rational number and therefore also rational

$$x = \frac{b_1 b_2 \dots b_m}{10^{k+m} - 1} + \frac{a_n \dots a_0 a'_1 \dots a'_k}{10^k} = \frac{10^k b_1 b_2 \dots b_m + (10^{m+k} - 1) a_n \dots a_0 a'_1 \dots a'_k}{10^{m+2k} - 10^k}$$

□

Let us now see that any real number can be assigned a decimal expression in a natural way. How could we get a decimal expansion for one equivalence class of sequences of rational numbers? The idea is that terms of a Cauchy sequence are very close to each other and that terms of equivalent sequences are also very close to each other. We can exploit this as follows: Choose a real number $[(a_n)]$, that is, an equivalence class of Cauchy sequences of rational numbers. We want to see first that the k^{th} decimal digit of a_n is fixed for n sufficiently large From the definition of Cauchy sequence, for each choice of k, there exists $m \in \mathbb{N}$ such that if $n_1, n_2 \geq m$ then $|a_{n_1} - a_{n_2}| < \frac{1}{10^k + 1}$ Therefore the first k digits of a_{n_1} and a_{n_2} coincide. We

can then define the decimal expression for the real number as the expression in digits that stabilizes.

We should check that this definition does not depend on the choice of the representative of the sequence (a_n). If we have another Cauchy sequence (a'_n) in the same equivalence class, $(a'_n) \sim (a_n)$ implies that for any k, there exists some $m \in \mathbb{N}$ such that if $n \geq m$ then $|a_n - a'_n| < \frac{1}{10^{k+1}}$. Therefore the first k digits of a_n and a'_n coincide, so the choice of decimal expression is independent of the representative.

We now check the properties of addition and product of real numbers:

Proposition 25.7. *Given Cauchy sequences $(a_n), (b_n), (c_n)$, the following properties are satisfied*

(a) $([(a_n)] + [(b_n)]) + [(c_n)] = [(a_n)] + ([(b_n)] + [(c_n)])$, $([(a_n)][(b_n)])[(c_n)] = [(a_n)]([(b_n)][(c_n)])$.
(b) $[(a_n)] + [(b_n)] = [(b_n)] + [(a_n)]$.
(c) $([(a_n)] + [(b_n)])[(c_n)] = [(a_n)][(c_n)] + [(b_n)][(c_n)]$.
(d) The coset of the constant sequence 0 is the set of sequences that have limit 0 and acts as the identity for addition $[(a_n)] + [(0)] = [(a_n)]$..
(e) If (a_n) is a Cauchy sequence, so is $(-a_n)$ and $[(a_n)] + [(-a_n)] = [(0)]$.
(f) The coset of the constant sequence 1 is the set of sequences that have limit 1 and acts as the identity for product $[(a_n)][(1)] = [(a_n)]$..
(g) If $[(a_n)] \neq 0$, then there exists some m such that either for all $n \geq m$ $a_n > 0$ or for all $n \geq m$ $a_n < 0$. Then a sequence (b_n) satisfying $b_n = \frac{1}{a_n}, n \geq m$ is a Cauchy sequence and $[(a_n)][(b_n)] = [(1)]$.

Proof. Most of the proofs are similar, so we only write a few. Try to write the rest on your own.

(c) Using the definition of addition of cosets of sequences

$$([(a_n)] + [(b_n)])[(c_n)] = ([(a_n + b_n)])[(c_n)] = [(a_n + b_n)c_n]]$$

Using the distributive property in the set of rational numbers $(a_n+b_n)c_n = a_nc_n+b_nc_n$ then using again the definition of addition and product of cosets of sequences,

$$[(a_nc_n + b_nc_n)] = [(a_nc_n)] + [(b_nc_n)] = [(a_n)][(c_n)] + [(b_n)][(c_n)]$$

(g) The condition $[(a_n)] \neq 0$ means that $\lim_{n\to\infty}(a_n) \neq 0$. Let us first write the condition $\lim_{n\to\infty}(a_n) = 0$. this would mean that

$$\forall \epsilon > 0,\ \exists m \in \mathbb{N} \text{ such that } \forall n \geq m,\ |a_n - 0| = |a_n| < \epsilon$$

The negation of this statement is

$$\exists \epsilon_0 > 0,\ \forall m \in \mathbb{N}\ \exists n \geq m,\ |a_n| > \epsilon \tag{1}$$

Let us now write the condition of Cauchy sequence for $\frac{\epsilon_0}{2}$

$$\exists m_1 \in \mathbb{N}, \forall n_1, n_2 \geq m, |a_{n_1} - a_{n_2}| < \frac{\epsilon_0}{2}$$

According to equation (1), we can find $n_1 > m_1$ such that $|a_{n_1}| > \epsilon$. Then, if $n_2 > m_1$, $|a_{n_1}| = |(a_{n_1} - a_{n_2}) + a_{n_2}| \leq |a_{n_1} - a_{n_2}| + |a_{n_2}|$. It follows that

$$|a_{n_2}| \geq |a_{n_1}| - |a_{n_1} - a_{n_2}| \geq \epsilon - \frac{\epsilon}{2} = \frac{\epsilon}{2} > 0.$$

Therefore $a_{n_2} \neq 0$. Define the sequence (b_n) by $b_n = \frac{1}{a_n},\ n \geq m_1, b_n = 1,\ n < m_1$ (we could define anything we want for $n < m_1$).

We need to check that (b_n) is a Cauchy sequence. From Proposition24.6, we can find a positive value A and some m such that for all $n \geq m, |a_n| \leq A$. Choose $\epsilon \in \mathbb{Q}^+$. There exists some $m_2 \in \mathbb{N}$ such that if $n_1, n_2 \geq m_2$, then $|a_{n_1} - a_{n_2}| \leq \frac{\epsilon}{A^2}$. Take $n_1, n_2 \geq \max\{m_1, m_2\}$, then

$$|b_{n_1} - b_{n_2}| = \left|\frac{1}{a_{n_1}} - \frac{1}{a_{n_2}}\right| = \left|\frac{a_{n_2} - a_{n_1}}{a_{n_1} a_{n_2}}\right| \leq \frac{\epsilon}{A^2} A^2 = \epsilon$$

So, (b_n) is a Cauchy sequence.

If $n \geq m_1,\ b_n = \frac{1}{a_n}$. Therefore $a_n b_n = 1, n \geq m_1$. As the coset of a Cauchy sequence only cares about what happens for n sufficiently large, $[(a_n)][(b_n)] = 1$.

□

Definition 25.8. Given Cauchy sequences $(a_n), (b_n)$, we write $[(a_n)] < [(b_n)]$ if and only if $[(a_n)] \neq [(b_n)]$ and there exists $m \in \mathbb{N}$ and for all $n \geq m$, $a_n < b_m$.

We should check that this is well defined and this is similar to the proof of Proposition 25.7(g).

We would also like to know that this is a total order rather than a partial one, that is

$$\forall (a_n), (b_n) \text{ Cauchy sequences , either } [(a_n)] < [(b_n)] \text{ or } [(a_n)] > [(b_n)] \text{ or } [(a_n)] = [(b_n)]$$

If you take two Cauchy sequences, the difference is a Cauchy sequence. We saw in Proposition 25.7(g) that if the coset of a sequence is not 0, then all the terms after a sufficiently large index are positive or all are negative. When you apply this result to the difference of two Cauchy sequences, you are showing that all the terms after a certain index of the first sequence are always smaller or always bigger than the second, which is the definition of inequality of sequences.

We would also like to have the rational numbers as a subset of the real numbers. We can do this as follows

Definition 25.9. Denote by (q) the constant sequence with all terms equal to q. Define $f : \mathbb{Q} \to \mathbb{R}$ by $f(q) = [(q)],\ \forall q \in \mathbb{Q}$,

The function f is one to one because if $q \neq q'$, the constant sequence $q - q'$ has limit $q - q' \neq 0$. Therefore, $[(q)] \neq [(q')]$. This allows us to identify $\mathbb{Q}$ with a subset of $\mathbb{R}$.

We can also define the absolute value of a real number by taking the sequence with absolute value of each given term

Definition 25.10. Given Cauchy sequences (a_n), we define the aboslute value by taking the Cauchy sequence of absolute values. $|[(a_n)]| = [|a_n|]$.

Of course, we would need to check that this is well defined. This means

- Checking that if (a_n) is a Cauchy sequence, then $(|a_n|)$ is a Cauchy sequence.
- Checking that if $(a_n), (a'_n)$ are Cauchy sequences with $(a_n) \sim (a'_n)$, then $(|a_n|) \sim (|a'_n|)$.

The usual properties of absolute value such as $|[(a_n)]| \geq 0, |[(-a_n)]| = |[(a_n)]|$ or $|[(a_n + b_n)]| \leq |[(a_n)]| + |[(b_n)]|$ are automatically satisfied from the same properties of absolute values in $\mathbb{Q}$.

Now that, once we have absolute values, we could define Cauchy sequences of real numbers. These are Cauchy sequences of Cauchy sequences! The most relevant point is that they are all convergent in $\mathbb{R}$, something that was not true in $\mathbb{Q}$.