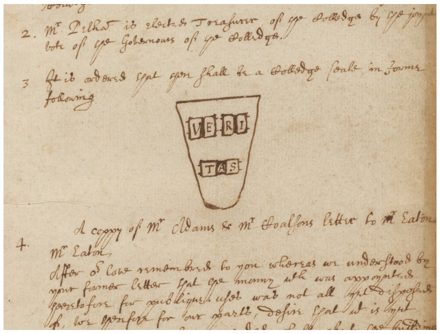
LINEAR ALGEBRA AND VECTOR ANALYSIS

MATH 22B

Unit 3: Definitions, Theorems and Proofs

Introduction

3.1. One of the truly amazing things about mathematics is that it is a frame work, where if something is established, it will remain truth for all eternity. The focus of most sciences changes rather quickly and frequently, entire paradigms change. Mathematics evolves too of course. But once established truths do not change. The theorem of Pythagoras we have proven in the first lecture is something which will still be true in a million years. The language how we describe a statement will almost certainly have completely changed in a future mathematical frame work. The statement of Pythagoras still will be valid.



2. Mr Pelham is elected Treasurer of ye Colledge by ye joynt vote of ye Governours of ye Colledge.

3 It is ordered that there shall be a Colledge seale in forme following

4. A copy of Mr Adams & Mr Coalsons letter to Mr Eaton

Mr Eaton,
After or Love remembred to you whereas we understood by your former letter that ye money wch was appoynted heretofore for publique use was not all [illegible] disposed of, we therefore for our parts, desire that wt is [illegible]

Figure 1. The first drawing of "Veritas". Veritas means "truth" Source: College Book 1, 1639-1795. UAI 5.5 Box 1, Harvard University Archives.

3.2. One of the most important sources for confusion are **sloppy definitions**. Mathematics has early on insisted on precise and unambiguous definitions. We have seen this in the first lecture. Defining a "vector" as a quantity with magnitude and direction is not only ambiguous and wrong (as it does not capture the zero vector), it lulls you into some sort of "understanding" as we all have intuition about magnitude like "length" and "direction" from daily life. It often happens even in "hard sciences" that sloppy definitions are used. Well, we have not be too arrogant. It turns out that coming up with precise and still elegant definitions is a rather difficult task in general. In physics, it took a long time to replace notions like "vis viva" and replace it with precise definitions like momentum or kinetic energy. It was Emily du Châtelet who essentially contributed to clear up the definitions and distinguish momentum mv and energy $mv^2/2$

3.3. The backbone of mathematics are the theorems. These are statement which have been verified using a careful sequence of arguments, where each step is either using a basic logical step or then uses a previously established theorem. It is extremely important not to have any wrong theorem in this process. Otherwise, everything which is built upon it will fall. Mathematics is like a big computer program in which the individual procedures are the theorems. If one of the procedures is faulty, it can bring down the entire system. There is always the risk that a proof will turn out to be incomplete or wrong and history has shown this to be the case again and again. Most of the time, one can fix the statement. Sometimes, one can not fix it because the statement has counter examples. In that case one has to modify the statement or adapt the definitions so that it becomes true. Lakatos has in his famous book "proofs and refutations" illustrated this in the context of the Euler Gem formula $V-E+F=2$ we have seen in the second lecture. This is a place where sloppy definitions for the notion of "polyhedron" led to wrong statements and the theorem had to be mended over time.

Lecture

3.4. **Theorems** are mathematical statements which can be verified by giving a proof. A **proof** assures that the theorem is true and remains valid also in the future. Let us look at an example of a theorem. It has already been known and proven by **Euclid of Alexandria**. It deals with **integers** and **primes**, positive integers larger than 1 which are only divisible by 1 or itself. The theorem tells that every positive integer is either 1 or prime or the product of two or more primes. To formulate the theorem more elegantly, we extend the notion of **product** and say that a prime is the product of $k=1$ primes and that the number 1 is a product of $k=0$ primes. Also we would say the number $20=2*2*5$ is the product of $k=3$ primes, even so the prime 2 appears twice. This is similar to the water molecule $H_2O=H*H*O$ containing $k=3$ atoms, as hydrogen H appears twice and oxygen O once. Now, like every molecule decomposes into atoms, every number decomposes into primes:

Theorem: "Every integer $n \geq 1$ is a product of $k \geq 0$ primes".

This is a remarkable statement because there are infinitely many integers. We can not go therefore through an infinite list and check things for each. It could a priori happen that for some very large number, like the **Fermat number** $F_{1000}=2^{(2^{1000})}+1$, which can not even be written down in our universe, [1] the statement would fail.

3.5. In order that such a statement can be verified or refuted, one needs first of all to make sure that the objects are described by **clear definitions**. In the above sentence, this means that we need to know what the "integers" are, what a "product" is and what "prime numbers" are. This is already tricky in general. Most confusions which have happened historically in science (and still today!) are based on sloppy definitions. [2]

[1] There are less than 2^{300} elementary particles available in our universe (as far as we know).

[2] Amuse yourself and try to find definitions of "entropy", "multiverse", "intelligence" or "life"

Problem A: Take your working definition of "natural number" and see whether the statement "every natural number is a finite sum of smaller rational numbers". You might want to compare with what a friend of yours thinks.

Problem B: Why is 1 not considered a prime number?

3.6. Once, the definitions of the ingredient of the statement is clear, it is helpful to clarify its **meaning**. We get intuition by looking at **examples**. We see for example that $100 = 2 * 2 * 5 * 5$ is indeed a product of prime numbers. We see also that 7 is a prime number. Examples are great but it is important at this stage to realize:

Principle: Checking a statement by showing a few examples is not a proof.

We will come back to this later in the course.

Problem C: The following statements are examples to theorems we have seen in the first two lectures:

Statement	Belongs to theorem
$3^2 + 4^2 = 5^2$	
$63 = [3,4] \cdot [5,12] \leq 5 * 13 = 65$	
$[0,1,0,0,1]$ can not be row reduced to $[0,0,1,1,0]$.	

3.7. One of the important proof techniques is the **principle of mathematical induction**. [3] It is mostly applied to integers but it can also be used for matrices as we have seen in the second lecture. The principle applies for statements $S(n)$ which depend on a number n.

Principle: $S(1)$ and $S(n) \Rightarrow S(n+1)$ implies $S(n)$ for all $n \geq 1$.

3.8. Here is an example:

Theorem: S(n): $1 + 2 + 3 + \cdots + n = (n^2 + n)/2$.

Proof: the statement $S(n)$ is true for $n = 1$. Assume $S(n)$ is true. Now $S(n+1)$ tells $1 + 2 + \cdots + n + (n+1) = ((n+1)^2 + (n+1))/2$. Using the induction assumption, this means $(n^2 + n)/2 + (n+1) = ((n+1)^2 + (n+1))/2$, which is true. We know therefore that the statement is true for all n.

[3] Already used by Plato and a second order axiom in the **Peano axiom system.**

3.9. Let us look at the theorem on primes above. In order to make this a statement which we can extend from n to $n+1$, we modify the statement to

Theorem: S(n): Every $k \in \{2, 3, 4 \cdots n\}$ has a prime factorization.

3.10. $S(2)$ is true as $\{2\}$ only contains one number which is prime. Now assume $S(n)$ meaning that the statement is true for n, prove that $S(n+1)$ is true. There are two cases: if $n+1$ is prime, then $S(n+1)$ is true. If $n+1$ is not prime, then $n = ab$ where a and b are numbers larger than 1 but smaller than n. By induction assumption, both a and b decay into primes: $a = p_1 p_2 \cdots, p_k$ and $b = q_1 q_2 \dots, q_l$ where p_j and q_j are primes. Therefore, $n+1 = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_l$.

3.11. It is important to understand the statement and not to overreach it. We have not proven that every integer has a **unique** decomposition into prime factors. This was not known by Euclid (who might not even have thought about it). It was only proven 2000 years later by Gauss. A common mistake which happens in mathematical proofs is that one cites a theorem which is known but over reaches its scope or then that one forgets one of the assumptions.

Principle: Do not extend the scope of an already established fact without justification.

3.12. If you think such mistakes happen to rookies only, this is not the case. Leonard Euler, probably the greatest mathematician of all times once attempted a proof of Fermat's last theorem by working with extended number systems like $\mathbb{Z}[\sqrt{-3}]$ which are all the numbers of the form $a + \sqrt{-3}b$, where a, b are integers. You see, one can add and multiply such numbers like integers and remain in the class. Euclid's proof also shows that there is a prime factorization. But there can be different prime factorizations. An example is $4 = 2 * 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$. A similar mistake was done by Gabriel Lamé who announced in 1847 a proof of Fermat's last theorem telling that for $n \geq 3$, no solutions to $x^n + y^n = z^n$ exist unless $xyz = 0$. Lamé's genius idea was to decompose $x^n + y^n$ into linear factors using numbers satisfying $\xi^n = 1$, so called **roots of unity**. Also here, Euclid shows that a prime factorization exists, but it is also here not unique. The mistake was actually quite important. It led to a "theory of ideals" by Ernst Kummer which allowed to prove Fermat's last theorem in certain cases.

Principle: Mistakes can open new doors and find ideas. A creative search process can lead to mistakes at first.

3.13. Of course, we have to try to avoid mistakes in the final product at all costs. Euler certainly earned the right to make some mistakes by creating a lot of mathematics, which will remain true for all eternity. But mistakes can be much more basic. Here is a beautiful example due to Polya: [5]

[4] see Mario Livio: Brilliant blunders, 2013

[5] George Polya: Induction and Analogy in Math, 1954 (Thanks to Jun Hou Fung for suggestion):

Theorem: S(n): In a collection of n horses, all have the same color.

Proof: The induction assumption is clear as for $n = 1$, all horses have the same color. Now assume that the statement is true for all groups of n horses. Take $n + 1$ horses and take the first away. These are n horses so that all have the same color. Now put the first back and take the last one away. Again we have n horses, so that all have the same color. Therefore all have the same color.

Problem D: What is wrong in the proof of Polya's horse theorem?

Here are some more amusements:

Theorem: Cats have nine tails.

3.14. Proof: No cat has no tail. A cat with a tail has a tail more than no cat. No cat has eight tails. Therefore, cats have nine tails.

3.15. For the following definition of "Prime numbers" we follow [6]:

A prime is a number with no divisors.
Boxes of chocolates always contain a prime number
so that, whatever the number of people present
somebody has to have that one left over.

3.16. Why do we start to do induction at $n = 1$ and not from the other end? The following song explains why: (just as a bit of background to appreciate the song: Aleph-Null = $\aleph_0$ is the cardinality of the **natural numbers** $\mathbb{N}$. $\aleph_1$ is the next larger cardinality. The cardinality of the **real numbers** $\mathbb{R}$ is $2^{\aleph_0}$ (as the Cantor diagonal argument shows that the real numbers can not be counted) which is the cardinality of all subsets of natural numbers. Cantor had shown that there are different infinities. A beautiful mind like Cantor's of course asked whether there is an infinity in between these two infinities.

The statement $2^{\aleph_0} = \aleph_1$ is the **continuum hypothesis** abbreviated CH. Work of Paul Cohen and Kurt Gödel in the sixties shows that one can not prove the statement nor its negation from ZFC set theory (an axiom system of our standard mathematics from which one can derive the Peano axioms including the principle of induction). Cantor had for a long time tried to prove CH, in vain. We know now that his efforts to prove this were doomed from the beginning. This possibility always exists. There is the possibility (very unlikely although) that we can not prove that every even number larger than 2 is a sum of two primes, even in the case if it would be true! [7]. The continuum hypothesis problem had been the first of Hilbert's problems of 1900.

Aleph-null bottles of beer on the wall,
Aleph-null bottles of beer,
You take one down, and pass it around,
Aleph-null bottles of beer on the wall.

[6] R. Ainsley: "Bluff your way in maths, 1990"

[7] See Apostolos Doxiadis: Uncle Petros and the Goldbach conjecture, Novel of 1992

3.17. And here is another Ainsley quote:

At the end of a proof you write Q.E.D,
which stands not for
Quod Erat Demonstrandum
as the books would have you believe, but
for Quite Easily Done.

Homework

Problem 3.1 Write down a proof by induction showing that $1+3+5+7+\cdots+(2n-1)=n^2$ for every integer $n \geq 1$.

Problem 3.2 Given a $n \times n$ matrix A, its **trace** is defined as the sum of the diagonal elements $\sum_k A_{kk}$. We can define in $M(n,m)$ the inner product $\mathrm{tr}(A^T B)$. First check that this inner product makes sense and that $A^T B$ is indeed a square matrix. Repeat each step of the proof of the Cauchy-Schwarz inequality and see that it still works.

Problem 3.3 Let us define a vector $v \star w = (v \cdot w)v/|v|^2$. It is called the **vector projection** of w onto v.
a) Is the operation $\star$ commutative?
b) Is the operation $\star$ associative?
c) Verify that v is perpendicular to $w-(v \star w)$.

Problem 3.4 Try to design yourself an elementary geometric proof of the Pythagorean theorem which does not use any algebra. First try this without looking it up. Then look up one the many proofs available and pick the one you like most and write or draw it out.

Problem 3.5 Given a $n \times m$ matrix A, assume that $\mathrm{rref}(A)$ has r leading 1 and that $\mathrm{rref}([A|b])$ has s leading 1. What condition on r and s and n and m implies that the system of equations $Ax=b$ has no solution? Experiment first with small examples.