Intuitive but rarely proven theorems and their applications

Marián Gloser

August 15, 2020

Abstract

In this paper we present some intuitive theorems, their proofs and their useful and surprising applications. The theorems presented here are not connected in any particular way and their choice is due to the author.

Introduction

As stated in the title the theorems in this paper are intuitive and thus rather trivial. By intuitive we mean that they are obviously true. We present their proofs nonetheless since the theorems are in most cases presumed to be proven beforehand. Some of these theorems may in fact be famous but may be interesting and have equally interesting applications so the author chose to include them in the paper.

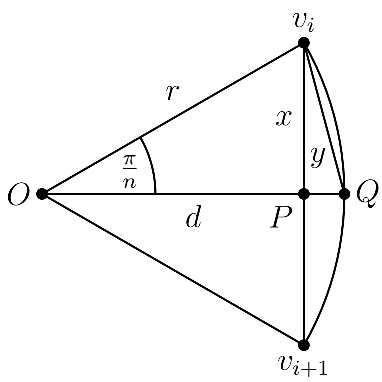
1 Circle as a limit of regular polygons

We define a circle as a set of points equidistant from another point called the centre of a circle. The limit of regular n-gon (set of all points on a circle for which the angle between horizontal line and line connecting the centre of the circle and the point on the circle is a multiple of $\frac{2\pi}{n}$ (vertices of the polygon), such that each vertex is connected to a vertex closest to it by a line segment) as n goes to infinity intuitively forms a circle. We have thus the following theorem.

Theorem 1. *The limit of regular n-gon as n goes to infinity forms a circle.*

Firstly, we have to define what we even mean by 'the limit of a regular n-gon'. For simplicity we will denote the circle as C and a regular n-gon inscribed in the circle as P_n. We say that P_n tends to C if for any positive real ϵ there exists an N such that for all $n \geq N$ we have: for each point of C there is a point of P_n at distance at most ϵ from it, and also for each point of P_n there is a point of C at distance at most ϵ from it. We will now give a proof of theorem 1.

Proof. Because of symmetry we can without loss of generality only consider points between 2 consecutive vertices of the polygon. We shall call these vertices v_i, v_{i+1}.



On the polygon we consider the midpoint of the side v_iv_{i+1} (labelled P in the diagram). Distance to any point of the arc v_iv_{i+1} is bounded by distance $|v_iP|$ which we will call x. Now if we look at the triangle OPv_i, we see that $x = r \sin \frac{\pi}{n}$. This distance goes to 0 in the limit as n goes to infinity, hence the distance from P to the circle eventually becomes less than any positive real ϵ.

Similarly on the circle we choose the midpoint of the arc v_iv_{i+1} (labelled Q in the diagram). Then the distance to any point of the polygon is bounded by $|Qv_i|$, which we will call y. We can see that the triangle OQv_i is isosceles

and that the angle at the vertex O is $\frac{\pi}{n}$. We can thus easily deduce that the angle OQv_i is equal to $\frac{\pi}{2} - \frac{\pi}{2n}$.
If we now consider the triangle PQv_i, we can get an expression for y.

$$y = \frac{x}{\sin(\frac{\pi}{2} - \frac{\pi}{2n})} = \frac{x}{\cos(\frac{\pi}{2n})} = \frac{r\sin(\frac{\pi}{n})}{\cos(\frac{\pi}{2n})}.$$

Using a double-angle formula for sine we get

$$y = \frac{r\sin(\frac{\pi}{n})}{\cos(\frac{\pi}{2n})} = \frac{2r\sin(\frac{\pi}{2n})\cos(\frac{\pi}{2n})}{\cos(\frac{\pi}{2n})} = 2r\sin(\frac{\pi}{2n}).$$

This distance also goes to 0 in the limit as n goes to infinity, hence the distance Q to the polygon eventually becomes less than any positive real ϵ and therefore the limit of regular n-gon as n goes to infinity converges to a circle. $\square$

If for every n the area of a polygon is defined, we can using this theorem very easily calculate the area of a circle. We will calculate the area of a polygon and using theorem 1 we shall get the formula for calculating the area of a circle. We see that the area of the triangle in the above diagram is obviously xd (d is the distance from O to P). Moreover there are n such triangles. So the area is

$$\lim_{n\to\infty} nxd = \lim_{n\to\infty} nr^2 \sin(\frac{\pi}{n})\cos(\frac{\pi}{n}) =$$
$$\lim_{n\to\infty} \pi r^2 \frac{\sin\frac{\pi}{n}}{\frac{\pi}{n}}\cos(\frac{\pi}{n}) = \lim_{n\to\infty} \pi r^2 \cos(\frac{\pi}{n}) = \pi r^2.$$

Normally we would have to show that the missing area between the polygon and the circle goes to zero. However here we have proven a theorem which enables us to calculate the area directly since the polygon becomes the circle.

2 Polygons can be decomposed into triangles

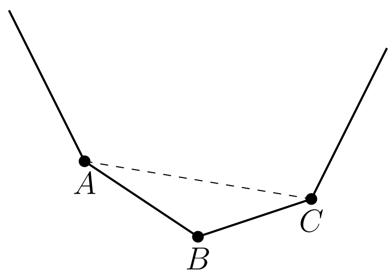
We will be concerned by the following theorem.

Theorem 2. *Every polygon can be decomposed into triangles.*

By decomposition into triangles we mean using straight lines to cut the polygon into a set of disjunct triangles (apart from common edges). In fact we shall prove a slightly stronger result: every polygon can be decomposed into triangles whose vertices are vertices of the polygon. The proof is quite straightforward. To begin we are going to prove the following lemma.

Lemma. *Every polygon has at least 1 convex ($< 180°$) angle.*

Proof. We proceed by induction. The base case is a triangle for which the lemma obviously holds. Suppose now that it holds for some n. We are going to prove that it holds then also for $n + 1$. Given an $(n + 1)$-gon we choose some 3 consecutive vertices (since the base case has 3 vertices, we can do this). Either at least one of them is convex, in which case we are done or none of them is convex.



In this picture interior angles of the polygon are the ones which are not convex. Consider now a new polygon consisting of the same vertices as the original one except it does not have the vertex B and vertices A and C are connected. Obviously, angles at vertices A, C remain bigger than $180°$. This polygon has n vertices and thus by induction hypothesis has at least one convex angle. Since it cannot be any of the angles at vertices A or C and the rest of the vertices is common with vertices of the original polygon, the $(n + 1)$-gon also has at least 1 convex angle. □

Proof of theorem 2 is very similar.

Proof. We proceed by strong induction. Case of a triangle is trivial. Consider it holds for all polygons up until some n-gon. When considering the case $n + 1$ we know by the lemma we have proven earlier that it has at least one convex angle. Either we can cut out a triangle formed by this angle and two adjacent vertices, or such a triangle intersects the polygon. In first case we are left with a polygon with n sides which by the induction hypothesis can be decomposed into triangles. In second case we simply form a diagonal with one vertex enclosed in the triangle and one vertex of the triangle. We cut the polygon along this diagonal to form 2 smaller polygons which can be decomposed into triangles by induction hypothesis. $\square$

Although the theorem is fairly trivial, it can prove to be quite useful. In fact, it is one of the key steps (although often just assumed true) when proving Wallace–Bolyai–Gerwien theorem (two polygons with the same area are equidecomposable).

3 Derivatives and inequalities

In this section we are going to state and prove one very intuitive theorem. The theorem is trivial, yet surprisingly useful when solving certain inequalities so it is quite a mystery why it is used so rarely. Throughout this section we will assume that $f(x), g(x)$ and their derivatives are Riemann integrable.

As the name of the section suggests, we will be dealing with derivatives and inequalities. Intuitively, if two functions at some point cross and one of them has bigger derivative, then that function is going to be bigger than the other one. Writing it more rigorously we get:

Theorem 3. *Suppose that $f(x_0) > g(x_0)$, $x_0 \in \mathbb{R}$ and that for $x > x_0$: $f'(x) > g'(x)$. Then $f(x) > g(x)$ for all $x > x_0$.*

In the proof we will use another theorem:

Theorem 4. *If $f(x) > 0$ for $b \geq x \geq a$, then $\int_a^b f(x)dx > 0$.*

Proof. We claim that if $f(x) > 0$ for $b \geq x \geq a$, then there exists an interval α contained in interval $[a, b]$ and a positive $M \in \mathbb{R}$, such that $f(x) > M > 0$ in interval α. We will prove this by contradiction.

Suppose on the contrary that for all intervals $\alpha \in [a, b]$ we have $f(x) \leq M$ for all positive real M. Since $f(x) > 0$ we can choose some $x_0 \in [a, b]$, such that $f(x_0) > 0$. It has to hold that $f(x_0) \leq M$. But if it holds for all positive real M, then it also should hold for $M = \frac{f(x_0)}{2}$, which is obviously not true.

We can now split the integral.

$$\int_a^b f(x)dx = \int_a^{\inf(\alpha)} f(x)dx + \int_\alpha f(x)dx + \int_{\sup(\alpha)}^b f(x)dx. \tag{1}$$

All the integrals in (1) can be written as $\lim_{n\to\infty} \sum_{k=0}^n f(x_k^*)\Delta x_k$ (function is Riemann integrable). Since each of the terms is ≥ 0 (Δx_k goes to 0 for each k as n goes to infinity) we have

$$\lim_{n\to\infty} \sum_{k=0}^n f(x_k^*)\Delta x_k \geq \lim_{n\to\infty} f(x_0^*)\Delta x_0 = 0.$$

It follows that

$$\int_a^b f(x)dx = \int_a^{\inf(\alpha)} f(x)dx + \int_\alpha f(x)dx + \int_{\sup(\alpha)}^b f(x)dx \geq \int_\alpha f(x)dx.$$

However $f(x) > M > 0$, so we can write

$$\int_\alpha f(x)dx = \lim_{n\to\infty} \sum_{k=0}^n f(x_k^*)\Delta x_k > \lim_{n\to\infty} \sum_{k=0}^n M\Delta x_k = M \lim_{n\to\infty} \sum_{k=0}^n \Delta x_k = M|\alpha| > 0.$$

Here $|\alpha|$ is the length of interval α. We have thus proven

$$\int_a^b f(x)dx > 0.$$

□

To prove theorem 3 we now need a lemma.

Lemma. *If $f(x) > g(x)$ in some interval $[a, b]$, where a can be $-\infty$ and b can be ∞, then $\int_a^b f(x)dx > \int_a^b g(x)dx$.*

Proof. Define $h(x) = f(x) - g(x) > 0$. Using theorem 4 we deduce

$$\int_a^b h(x)dx = \int_a^b f(x)dx - \int_a^b g(x)dx > 0 \implies \int_a^b f(x)dx > \int_a^b g(x)dx.$$

□

Proof of theorem 3 is now very easy.

Proof. Since $f'(x) > g'(x)$, we deduce using the lemma and the Fundamental Theorem of Calculus that $f(x) > g(x) + f(x_0) - g(x_0) > g(x)$. □

4 Unsolvability of 5th degree polynomial equations implies unsolvability of equations of higher degree

A famous result of algebra is the Abel-Ruffini theorem which states that a polynomial equation of 5th degree with integer coefficients: $x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$, cannot be solved algebraically. Naturally, we expect also equations of higher degree to be unsolvable as well. In fact, this is true as we shall prove in this section.

Theorem 5. *Unsolvability of d-th degree polynomial equations implies unsolvability of equations of higher degree.*

The proof is quite trivial. However in order to prove this we have to be more precise. We say an equation is algebraically solvable if there exists an algebraic function of the coefficients of a given equation which gives the roots of the equation. That does not mean that equations of 5th and higher degree cannot be solved by other than algebraic means. It only happens to be true that equations of 5th degree are algebraically unsolvable and thus are also equations of higher degree.

Proof. Suppose that equations of some degree d cannot be solved algebraically. Now suppose that equation of some degree $n > d$ can be solved algebraically.

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0, \quad a_n \neq 0. \tag{2}$$

Then there exists an algebraic function $f(a_n, a_{n-1}, ...a_0)$, which gives all the roots of (1). We now set $a_0, a_1, ...a_{n-d-1}$ to be equal to 0. We get

$$\begin{aligned} &a_n x^n + a_{n-1}x^{n-1} + \cdots + a_{n-d+1}x^{n-d+1} + a_{n-d}x^{n-d} = \\ &\quad x^{n-d}(a_n x^d + a_{n-1}x^{d-1} + \cdots + a_{n-d+1}x + a_{n-d}) = 0. \end{aligned} \tag{3}$$

Equation (2) has an arbitrary equation of d-th degree as a factor. The function f gives the roots of equation (2) and consequently the roots of an equation of d-th degree with an additional root 0 if $a_n \neq 0$. That implies that also equations of degree d are algebraically solvable, which is a contradiction. $\square$

5 Every polynomial of degree n has at most n roots

In this section we are going to prove the following theorem. We will be working over complex numbers.

Theorem 6. *Every polynomial of degree n has at most n roots.*

The theorem seems obvious to such an extent that one would be tempted to state instead that every polynomial of degree n has exactly n roots (counting in repeated roots). This is of course true, but is a lot harder to prove because it is a consequence of this theorem and another theorem, namely The Fundamental Theorem of Algebra which guarantees existence of at least one root. And that is much harder to prove.

Proof. We proceed by induction. Clearly, if $n = 1$, the theorem holds. Assume it holds for some n. We now consider some polynomial $p(x)$, where $\deg(p) = n+1$. Either the polynomial has no solutions, in which case we the theorem holds or assume it has a solution (say $x = a$). Then by Euclidean division for polynomials there exist polynomials $q(x), r(x)$, such that

$$p(x) = q(x)(x - a) + r(x),$$

where $\deg(q) = n$ and $\deg(r) = 0$. Notice that $p(a) = 0$ and so $r(a) = 0$, but $r(x)$ is a constant, so we get $r(x) = 0$. Hence

$$p(x) = q(x)(x - a).$$

Since by induction hypothesis $q(x)$ has at most n roots, $p(x)$ has the same roots and an additional root $x = a$. Hence $p(x)$ has at most $n + 1$ roots. □

Note that if polynomials have at least one root (in other words, assuming The Fundamental Theorem of Algebra holds), then a polynomial $p(x)$ can thus be written like this

$$p(x) = q(x)(x - a_1).$$

Where $\deg(p) = n$ and $\deg(q) = n - 1$. Now $q(x)$ has a root, so

$$q(x) = r(x)(x - a_1)(x - a_2).$$

Here $\deg(r) = n-2$. Continuing this process and applying theorem 5 we get

$$p(x) = (x - a_1)(x - a_2) \dots (x - a_n).$$

Since The Fundamental Theorem of Algebra holds, we get its equivalent

Theorem 7. *Every polynomial of degree n has exactly n roots (counting in repeated roots).*[1]

[1] If a polynomial $p(x) = (x - a)^m q(x)$, where $q(a) \neq 0$, then we say a is a root of multiplicity m. Roots of multiplicity ≥ 2 are called repeated roots.