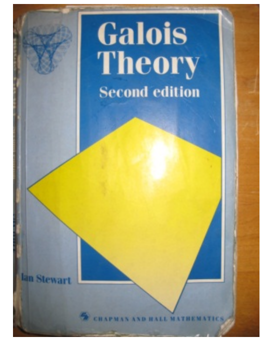
Joseph Liouville's construction of a transcendental number

Joseph Liouville

Topmatter:

Some ideas pulled from exercises 6.6 – 6.8 in *Galois Theory* (Second Edition) by Ian Stewart, page 69, some from elsewhere.

Here, present a (probably modified) version of the work of the French mathematician Liouville that explicitly made a transcendental number, and some work that was done after his of 1844. The number here produced is Liouville's Constant. The later work of the German mathematician Cantor made no transcendental numbers, but had significant ideas of cardinality.



My beat-up text

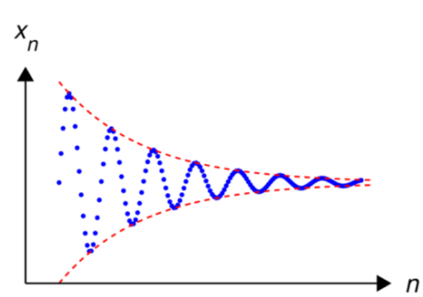
There are countless web references to transcendental numbers, a Wikipedia page. There are biographies of Joseph Liouville, discussions of transcendental numbers, and even a page on the "fifteen most famous transcendental numbers." But could not find a good construction, though this page has some discussion on a higher level than this one, as does this link.

Credit:

Slowly typeset by Dean Moore, October – December 2010, Boulder, Colorado, USA, tweaks afterward. Did some notable fixes in September 2016, improving explanations, fixing confusing math and mistakes, plus bad notation, a couple of holes, general nonsense. Also did fixes, June 2017.

In March 2009, worked the proof for pure entertainment, later typeset to slowly piece through, to understand the logic, and fill in gaps. Parts are my revenge against math texts, where the passage "Thus it clearly follows …" was found, and hours of work was required to fill in the abyss between "clearly" and "follows." Why in graduate school at CU – Boulder a mathematician studying analysis bought a book on Galois Theory—which lands in the basket of abstract algebra—is a hidden mystery, though years later worked through it. Fascinating material, Galois Theory.

Here, aim at a simplistic explanation with many references (probably too many) that could be understood by an undergrad in math with some understanding of real analysis, number theory, rings and fields, a little set theory. You are expected to have familiarity with elementary algebra as exponents. Some understanding of limits of sequences and infinite sums is a must. Understanding of some mathematical notation is assumed; one reference is here. A few relevant terms:



Basic understanding of limits of sequences is a must, as is some understanding of series.

- $\forall$ means "For all,"
- $\exists$ means "There exists,"
- ϵ means "Is an element of," and

- $\{0, \ldots n\}$ is a "set notation," here means "The set of all integers from 0 to n, inclusively."
- "Pass to a subsequence" means, of say, a sequence like $\left\{\frac{p_i}{q_i}\right\}_{i=1}^{\infty}$ to choose a new sequence by throwing out a subset of $\left\{\frac{p_i}{q_i}\right\}_{i=1}^{\infty}$. This is written $\left\{\frac{p_{i_j}}{q_{i_j}}\right\}_{j=1}^{\infty}$ and note, i_j refers to a subset of all i, now indexed by j. Notably, when $\lim_{i\to\infty} \frac{p_i}{q_i} = \frac{p}{q}$, it is also true that $\lim_{j\to\infty} \frac{p_{i_j}}{q_{i_j}} = \frac{p}{q}$.

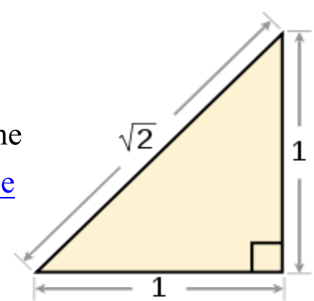
Images tend to be Wikipedia images. If by some weirdness someone finds it useful, great. Send me an e-mail, *dean* at *deanlm* dot *com*, or if made some typo, flub or poor logic.

Background:

Rational numbers, the ancient Greeks:

Ancient Greek mathematicians first assumed all numbers rational, i.e., ratios of integers as $\frac{p}{q}$, with $p, q \in \mathbb{Z}, q \neq 0$. Easy examples are

$$y_0 = \frac{5}{7}, y_1 = \frac{13}{1} = 13, \text{or } y_3 = \frac{3^2 \cdot 7 \cdot 127 \cdot 7853}{2^8 \cdot 5^7} = 3.14159265$$



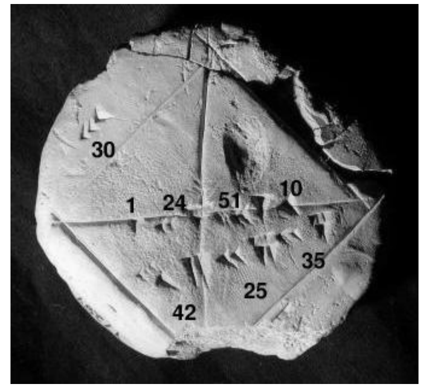
The Greeks knew of the square root of two, $\sqrt{2}$, from obvious considerations from the Pythagorean Theorem (diagram, right: Note $\sqrt{2}$ is the hypotenuse of the right triangle with both short legs of length 1, as $1^2 + 1^2 = 2$). Initially, they assumed $\sqrt{2}$ rational. Eventually, a Greek proved the square root of two was *irrational*, i.e., cannot be expressed as a fraction of two integers. This has been proved, in many ways.

So for $p, q \in \mathbb{Z}, q \neq 0$ to write

$$\frac{p}{q} = \sqrt{2}$$

is impossible. As rational numbers are dense in the real line, one may use rational numbers to get arbitrarily "close" (i.e., limit), but *equality* cannot happen.

Notably for the polynomial $f(x) = x^2 - 2$, the numbers $x_2 = -\sqrt{2}$ and $x_3 = \sqrt{2}$ satisfy $f(x_2) = f(x_3) = 0$. So $\pm\sqrt{2}$ are the roots of a polynomial in rational (here integer) coefficients.



***Babylonian mathematics* on $\sqrt{2}$.**

So we have an simple way to include numbers like $\sqrt{2}$ in our number system and in terms of simple familiar things: roots of polynomials in integer coefficients, ideas studied since at least the ancient Egyptians and Babylonians.

Algebraic numbers:

Thus algebraic numbers: all numbers—real or complex, but this paper stays in the world of real numbers—that are roots of some polynomial

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} + a_n x^n,$$

$$n \in \mathbb{N};\ a_i \in \mathbb{Q}, \forall\, i \in \{0, \ldots n\}$$

The French mathematician Évariste Galois, at roughly the age of 15. He had about five years to live, but before dying solved a problem that had been floating around for hundreds of years. Galois was brilliant, changed mathematics forever, but lived a sad, rather tragic life.

in rational coefficients (equivalently, integer: since $f(x)$ is set equal zero one may multiply by a least common multiple to make all coefficients integers). That these form an algebraically closed field is proven elsewhere. This result is in various books; some discussion here. As an example, a number as

$$\frac{\left(3 + 7^{\frac{3}{17}}\right)^{\frac{11}{5}}}{\left(5^{\frac{7}{2}} - 2^{\frac{1}{4}} + 1\right)^{\frac{52}{73}} - 1}$$

is algebraic, a root of some integer–coefficient polynomial. From Galois Theory, roots of polynomials of degree five and higher cannot, in general, be expressed as combinations of radicals of integers or rational numbers, as in general, such polynomials are "not solvable." But Galois Theory gets a bit away from the subject matter of this paper.

Mainly as it's impossible, no one *proved* all numbers are algebraic. After Liouville's work of 1844, in 1874 Georg Cantor proved the algebraic numbers a field of cardinality $\aleph_0$, actually small in a set–theoretic sense, the first infinity. The real

Georg Cantor, whose theorems are now at the foundation of mathematics, but who in his life saw his ideas experience ferocious opposition, notably from Leopold Kronecker and Henri Poincaré

numbers—or the complexes—are fields of cardinality $2^{\aleph_0}$. Note $2^{\aleph_0}$ is sometimes equated to $\aleph_1$, but this is set theory and not currently decidable, and gets afield for this paper. Here $2^{\aleph_0}$ means "the second infinity," which is strictly larger than $\aleph_0$. But cardinality waited for Cantor, whose work postdated Liouville.

The transcendental numbers:

Algebraic numbers led to the idea of the *transcendental number*: a number—real or complex—that is not the root of any polynomial with rational (equivalent, integer) coefficients or algebraic coefficients—the algebraic numbers are algebraically closed, so algebraic coefficients is the same as to integer coefficients. Algebraically closed fields also get a bit afield, for the paper.

That is to say, a transcendental number equals any number—real or complex—that is not algebraic. It is easy to *talk* about such an idea, as a *theoretical* construct.

However, no one explicitly *constructed* one, though in 1677 the mathematician James Gregory attempted to prove π transcendental (this history here and here). The term *transcendental* goes back to at least Leibniz in 1673, if more modern formulations appear to trace to Euler in 1748.

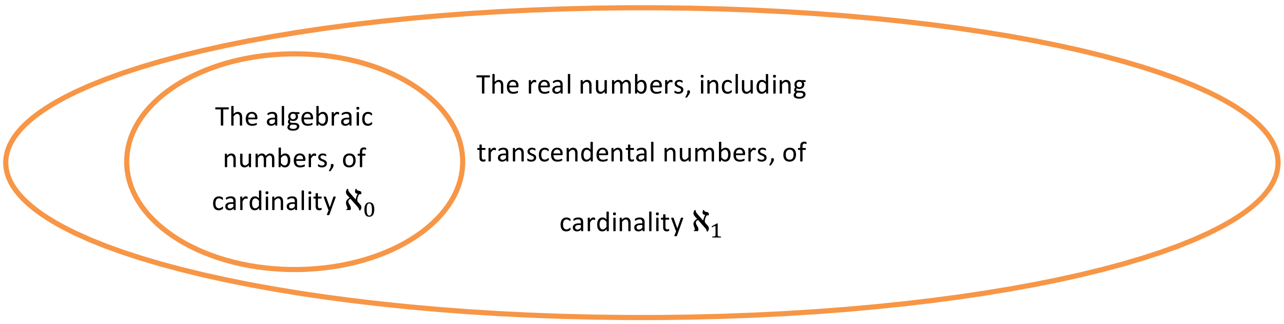
Genesis: Transcendental numbers were first proven to exist in 1844 by the French mathematician Joseph Liouville, though he did not then construct an explicit decimal number but a continued fraction. The first *decimal* proven transcendental was the Liouville constant which Liouville proved transcendental in 1850, not 1844 as stated in some web references. It belongs to a class of numbers, a "Liouville number," is a bit odd, and never occurs in physics. The first "naturally" occurring transcendental numbers were later proven to be *e* (Hermite, 1873) and *π* (Lindemann, 1882), neither of which are Liouville numbers.

As an aside, when in 1882 the number π was proven transcendental, it proved that by the methods of ancient Greek geometers it is impossible to square the circle. This answered a question had been open for thousands of years.

After Liouville, Cantor discovered no transcendental numbers but showed they had to exist, and his work had significant implications of cardinality: Via his "diagonal argument," Cantor showed the real numbers comprise a "big" uncountable $2^{\aleph_0}$ set. Cantor also showed the algebraic numbers are a countable set, that is, are of the cardinality called "countable infinity." As

- the algebraic numbers are *countable*, and no transcendental number is algebraic, *and*
- the real numbers are *uncountable*,

it follows that transcendental numbers must comprise an uncountable set, that is, a "big" set of cardinality $2^{\aleph_0}$, not a "small" set of cardinality $\aleph_0$. In terms of describing cardinality with different–sized blobs, the following Venn diagram is inaccurate, as the measure of the algebraic numbers equals zero, thus algebraic numbers should be an invisible dot. But it gives some idea:



A foretaste of what is to come:

Let x_0 be an irrational algebraic number, a root of a polynomial $f(x) \epsilon \mathbb{Z}[x]$ of degree n. In this foretaste, we fix x_0. Liouville took n, and bounds of the derivative of f "near" x_0, and set a "speed limit" on how fast a sequence of rational numbers can limit on an irrational algebraic number. We will set up this speed limit.

Using that speed limit, Liouville then showed only a finite set of rational numbers could beat a stronger speed limit to x_0. We will set up this speed limit.

He defined a new irrational number we will define. He set up a sequence of rational numbers limiting to this new irrational number. He then proved an *infinite* subset of the sequence broke the strong speed limit, when he had proved that only a *finite* set could break his "speed limit." So the limit could not be an algebraic number. Hence, the limit number was transcendental.

Construction of a transcendental number:

To do in detail, the construction is long and tedious with a few proofs. First we define a few things.

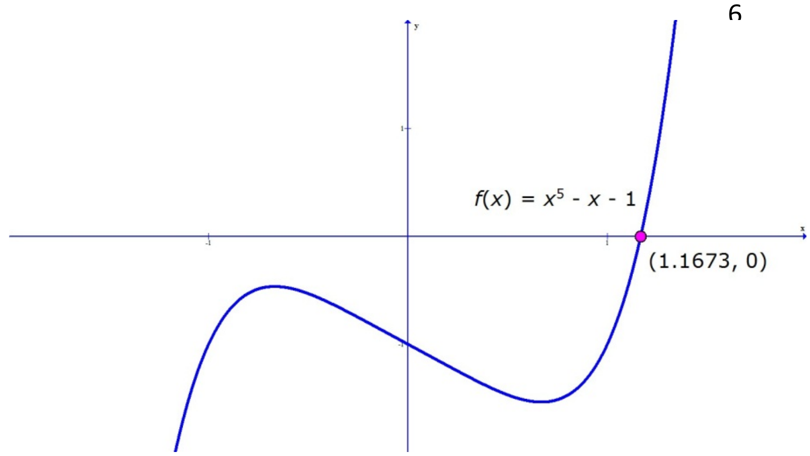
Definition 1

Let $\mathbb{Z}[x]$ be polynomials, with all coefficients in $\mathbb{Z}$. For this entire paper, all polynomials have coefficients in $\mathbb{Z}$.

Definition 2

Suppose we have an $n_{th}-$degree polynomial $f(x)\,\epsilon\,\mathbb{Z}[x]$ not identical zero (i.e., $n \geq 1$). Notably Lemma 7 and all else below depends on the polynomial having coefficients in $\mathbb{Z}$, equivalent to $\mathbb{Q}$. We henceforth assume this, so unless so identified, our polynomial is not assumed monic; it may look like $f(x) = -3x^5 + 19x^2 - 81$, not monic like

$$f(x) = x^5 - \frac{19}{3}x^2 + 27$$



Graph of the fifth-order polynomial $f(x) = x^5 - x - 1$. The lone real root at $x \approx 1.1673$ is a real algebraic; the other four roots are complex algebraic numbers. By Galois Theory, this polynomial is not "solvable" (mentioned here), so no roots may be obtained via algebra and extraction of roots on integers/rational numbers.

Our polynomial follows:

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1}x^{n-1} + a_n x^n,$$

$$n\,\epsilon\,\mathbb{N};\ a_i \epsilon\,\mathbb{Z}, \forall\, i\,\epsilon\,\{0, \dots n\};\ a_n \neq 0$$

Definition 3

Suppose $x_0\,\epsilon\,\mathbb{R} \backsim \mathbb{Q}$, and we have $f(x_0) = 0$, that is, x_0 equals an irrational algebraic number. We fix the number x_0 for the remainder of this paper.

Note we keep f fixed until Definition 17, will be referred to without redefinition.

Note when $n = 1$, x_0 is rational, the single zero of a polynomial like $f(x) = 2x - 9$, and every rational number is of degree 1; see Definition 4 direct below for a definition of "degree" when applied to a number. As x_0 is irrational, $\deg\big(f(x)\big) \geq 2$.

Definition 4

When x_0 equals an algebraic number and f is the minimal polynomial,—the monic polynomial of rational coefficients, of smallest degree of which x_0 is a root—n is called the *degree* of x_0; see also this link for a definition. Polynomials $g(x)$ of arbitrarily large degree satisfy $g(x_0) = 0$, but using a minimal polynomial can give better, larger bounds; see Lemma 7 below. As an example, $2^{\frac{1}{2}}$ equals a root of $f(x) = x^2 - 2$, so is "second degree." But $2^{\frac{1}{5}}$ equals a root of $g(x) = x^5 - 2$ and no polynomial in rational coefficients of lower degree than 5, so $2^{\frac{1}{5}}$ is fifth degree.

Henceforth can simply ignore the word "minimal," and all in this paper will work.

Definition 5

Note $n = \deg(f)$, the degree of f, will come up again.

Definition 6

In this entire paper, $p, q \in \mathbb{Z}, q \neq 0$, so p and q are always integers, and $\frac{p}{q}$ is always rational, as is $\frac{p_i}{q_i}$. In any fraction $\frac{p}{q}$, assume $q \geq 1$, as we can always move a negative sign to p.

Lemma 7.

Let polynomial $f(x) \in \mathbb{Z}[x]$ of be of degree n. If $p, q \in \mathbb{Z}, q \neq 0$ (assume $q \geq 1$, safe; see Definition 6) and $f\left(\frac{p}{q}\right) \neq 0$, it follows that $\left|f\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^n}$ is always true.

Proof.

As $f\left(\frac{p}{q}\right) \neq 0$ assume $f\left(\frac{p}{q}\right) = c \neq 0$. Note c is easily rational as f is a polynomial over $\mathbb{Z}$. So, $c \in \mathbb{Q} \backsim \{0\}$. Stating this,

$$f\left(\frac{p}{q}\right) = \sum_{i=0}^{n} a_i \left(\frac{p}{q}\right)^i = c$$

Taking absolute values of both sides we have:

$$\left|f\left(\frac{p}{q}\right)\right| = \left|\sum_{i=0}^{n} a_i \left(\frac{p}{q}\right)^i\right| = |c|$$

Now multiply both sides by q^n, which is positive, so it "filters through" absolute value brackets:

$$q^n|c| = q^n \left|f\left(\frac{p}{q}\right)\right| =$$

$$q^n \left|\sum_{i=0}^{n} a_i \left(\frac{p}{q}\right)^i\right| = \left|\sum_{i=0}^{n} a_i p^i \cdot q^{n-i}\right|$$

or,

$$q^n \cdot f\left(\frac{p}{q}\right) = \left|\sum_{i=0}^{n} a_i p^i \cdot q^{n-i}\right|$$

Note in bottom right sum that as $n - i \geq 0$ is always true, and $n - i$ always equals an integer. And as $a_i \epsilon\, \mathbb{Z}, \forall\, i,$ and $p, q\ \epsilon\ \mathbb{Z}$, all terms of above's bottom right sum are integers. So $q^n|c|$ equals some natural number, is in $\mathbb{N}$. In short, $q^n|c| \geq 1$.

Thus,

$$q^n \left| f\left(\frac{p}{q}\right) \right| \geq 1$$

Dividing by q^n we get $\left| f\left(\frac{p}{q}\right) \right| \geq \frac{1}{q^n}$. □

Example 8

As an example of the last, $x = \sqrt{2}$ satisfies $f(x) = x^2 - 2$. While $\sqrt{2} = 1.41421 \ldots$ is irrational, its digits never ending with no known pattern, we can approximate it with $\frac{p}{q} = \frac{141421}{10000} = \frac{7 \cdot 89 \cdot 227}{10000}$ (coprime form). So $q = 10000$. Note

$$\left| f\left(\frac{p}{q}\right) \right| = \left| \left(\frac{7\ \cdot\ 89\ \cdot\ 227}{10000}\right)^2 - 2 \right| \cong 1.00759 \cdot 10^{-5}$$

Note here $n = 2$ (the degree of $f(x) = x^2 - 2$), and $\frac{1}{q^2} = \frac{1}{10000^2} = 10^{-10}$, and as

$$1.00759 \cdot 10^{-5} \geq \frac{1}{10000^2} = 10^{-8}$$

that $\left| f\left(\frac{p}{q}\right) \right| \geq \frac{1}{q^n}$ seems obvious, by about three orders of magnitude.

Calculus Result 9

By the extreme value theorem of calculus, on a bounded interval the derivative $\frac{df}{dx}$ of the polynomial f is continuous, thus is bounded. Thus $\exists\ M\ \epsilon\ \mathbb{R}^+$ such that $\forall\ y\ \epsilon\ [x_0 - 1, x_0 + 1]$ we have $|f'(y)| \leq M$.

Discussion 10

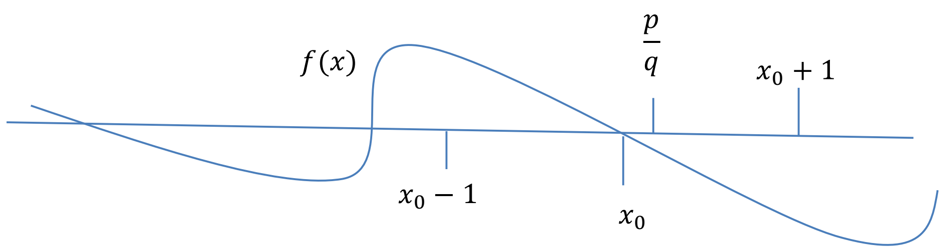
We will be looking at rational sequences $\left\{\frac{p_i}{q_i}\right\}_{i=1}^{\infty}$ with $\lim_{i \to \infty} \left(\frac{p_i}{q_i}\right) = x_0$. As the rational numbers are dense in the real line, such a sequence exists. So after a finite point all terms of such a sequence are in the interval $[x_0 - 1, x_0 + 1]$, and we can use Calculus Result 9.

Comment 11

Our next proposition will establish our first "speed limit." Of a rational number $\frac{p}{q}$, remember that for all irrational numbers x_0 that $\frac{p}{q} \neq x_0$ is always true.

Convention 12

For x_0 an irrational root of the polynomial $f(x) \in \mathbb{Z}[x]$, assume $\frac{p}{q} \in \mathbb{Q}$ is "close" to x_0 in the sense of $x_0 - 1 < \frac{p}{q} < x_0 + 1$, and that $\frac{p}{q}$ is closer to x_0 than any to other root of f. In a so–so graph:



In short, we want $f\left(\frac{p}{q}\right) \neq 0$, why $\frac{p}{q}$ is closer to x_0 than to any other root of $f(x)$.

We further comment, if $f(x)$ is a minimal polynomial—see Proposition 13 direct below—this convention is not needed. This is as a rational $\frac{p}{q}$ can't be a factor of a *minimal* $f(x)$ which has an irrational algebraic root x_0, as if $\frac{p}{q}$ is a root of $p(x) = a_0 + a_1 x + \cdots a_{n01} x^{n-1} + a_n x^n$, we can factor, and for $r(x)$, a degree $n-1$ polynomial, we could get $p(x) = r(x) \cdot (qx - p)$, and for x_0 we would have a new minimal polynomial $q(x)$, of lower degree; see Definition 4.

Proposition 13.

Using Calculus Result 9, we maintain that for any rational number $\frac{p}{q}$ which by Convention 12 is "near" our earlier–defined irrational x_0, a root of the n^{th}–degree minimal polynomial $f(x) \in \mathbb{Z}[x]$, that there exists an $M \in \mathbb{R}^{+}$ such that

$$\left|\frac{p}{q} - x_0\right| \geq \frac{1}{M \cdot q^n}$$

Proof.

In this proof it should be clear why having $f(x)$ be a minimal polynomial (see Definition 4) of x_0 works best, as the exponent n on $\frac{1}{q^n}$ is smallest, and $\frac{1}{M \cdot q^n}$ will be largest. All this may work, for a 100^{th}–order polynomial, but if we use the minimal polynomial which is, say, 5^{th}–order, we will get the largest bound.

We also point out, $f'(x_0) \neq 0$: If $f'(x_0) = 0$, that means x_0 is at least a double root of $f(x)$, which for a minimal polynomial doesn't make sense: Could differentiate $f(x)$, and have a polynomial of one less degree of which x_0 equals a root. So $M \geq |f'(x_0)| > 0$. In short, there is no "limiting out" of this proposition's conclusion.

To work: Let $f(x)$ be the minimal polynomial of x_0. Further let $M > 0$ be as in Calculus Result 9, that is, such that $\forall\, y \,\epsilon\, [x_0 - 1, x_0 + 1]$ we have $|f'(y)| \leq M$.

Note x_0 is irrational, so $\frac{p}{q} \neq x_0$ must be true. By Convention 6, $\frac{p}{q}$ is nearer to x_0 than to any other root of f, so $f\left(\frac{p}{q}\right) = 0$ is impossible. That $f\left(\frac{p}{q}\right) \neq 0$ will be of some importance.

By the Mean Value Theorem, between $\frac{p}{q}$ and x_0 the derivative f' of f assumes a "mean value," that is, $\exists\, c \,\epsilon \left(\min\left\{\frac{p}{q}, x_0\right\}, \max\left\{\frac{p}{q}, x_0\right\}\right)$ such that

$$\frac{f\left(\frac{p}{q}\right) - f(x_0)}{\frac{p}{q} - x_0} = f'(c)$$

As $f(x_0) = 0$, we may restate the left side,

$$\frac{f\left(\frac{p}{q}\right) - f(x_0)}{\frac{p}{q} - x_0} = \frac{f\left(\frac{p}{q}\right) - 0}{\frac{p}{q} - x_0}$$

Simplifying, and equating to the right side:

$$\frac{f\left(\frac{p}{q}\right)}{\frac{p}{q} - x_0} = f'(c)$$

Taking absolute values, from our chosen value of M in Calculus Result 9 this gives

$$\left|\frac{f\left(\frac{p}{q}\right)}{\frac{p}{q} - x_0}\right| = |f'(c)| \leq M$$

But from Proposition 13 we know that

$$\left|f\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^n}.$$

Aside: The last is where $f\left(\frac{p}{q}\right) \neq 0$ matters, a hypothesis of Proposition 13, and why we choose $\frac{p}{q}$ closer to x_0 than to any other root of f, as this renders $f\left(\frac{p}{q}\right) = 0$ impossible. All that truly matters is that $f\left(\frac{p}{q}\right) \neq 0$. It is also key that $f(x_0) = 0$, a hypothesis of this proposition.

Joining $\left|f\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^n}$ with $M \geq |f'(c)|$, and doing a little algebra

$$M \geq |f'(c)| = \left|\frac{f\left(\frac{p}{q}\right)}{\frac{p}{q} - x_0}\right|$$

$$= \left|f\left(\frac{p}{q}\right)\right| \cdot \left|\frac{1}{\frac{p}{q} - x_0}\right| \geq \left(\frac{1}{q^n}\right) \cdot \frac{1}{\left|\frac{p}{q} - x_0\right|}$$

Re-stating the top left and bottom right terms:

$$M \geq \left(\frac{1}{q^n}\right) \cdot \frac{1}{\left|\left(\frac{p}{q} - x_0\right)\right|}$$

We divide by M and multiply by $\frac{p}{q} - x_0$ to derive

$$\left|\frac{p}{q} - x_0\right| \geq \frac{1}{Mq^n}$$

This verifies our inequality, and establishes our first "speed limit." □

Discussion 14

We will be looking at rational sequences $\left\{\frac{p_i}{q_i}\right\}_{i=1}^{\infty}$ with $\lim_{i\to\infty} \frac{p_i}{q_i} = x_j$; we will later define x_1.

For an irrational algebraic x_0 for some "large" $i = i_0$ we have

- The sequence $\left\{\frac{p_i}{q_i}\right\}_{i=i_0}^{\infty} \epsilon\ (x_0 - 1, x_0 + 1), \forall\ i \geq i_0$, *and*
- some positive number M will be a bound of $\left|\frac{df}{dx}\right|$ on $[x_0 - 1, x_0 + 1]$, *and*

- Convention 12 will be true $\forall\ i \geq i_0$, *so*
- Proposition 13 will be true, $\forall\ i \geq i_0$.

Proposition 13 showed $\left|\frac{p}{q} - x_0\right|$ has to be bigger than something. The next proposition shows that for only a finite set of rational numbers can $\left|\frac{p}{q} - x_0\right|$ be smaller than a stronger bound, and matters in Theorem 18 that proves the existence of a transcendental number.

We note the Thue–Siegel–Roth theorem has stronger bounds than the next. Its proof is not easy, and led to a Fields Medal. What is relevant is that $k > n = \deg(f)$.

Proposition 15.

Let $f \in \mathbb{Z}[x]$ be the minimal polynomial of an irrational root x_0. Fix a real $K > 0$. Fix a natural number k such that

$$k > n = deg\ (f)$$

Let $\left\{\frac{p_i}{q_i}\right\}_{i=1}^{\infty}$ be an infinite set of unique rational numbers, that is, whenever $i \neq j$, we have

$$\frac{p_i}{q_i} \neq \frac{p_j}{q_j}$$

For some index set I there exists an at most finite set S of unique rational numbers,

$$S = \left\{\frac{p_i}{q_i}\ \middle|\ i \in I; p_i, q_i \in \mathbb{Z}, q_i \neq 0\right\}$$

such that

$$\left|\frac{p_i}{q_i} - x_0\right| < \frac{K}{q_i^k}$$

That is, the index set I is finite, hence S is a finite set. We assume $\{q_i \geq 1, \forall\ i \in I\}$; see Definition 6.

Proof.

We do a proof by contradiction. Assume for an infinite index set (as the rational numbers form an $\aleph_0$ set, we choose $I = \mathbb{N}$) there exists a set

$$S = \left\{\frac{p_i}{q_i}\ \middle|\ i \in \mathbb{N};\ p_i, \in \mathbb{Z}, q_i \in \mathbb{N}, \forall\ i\right\}$$

with each $\frac{p_i}{q_i}$ unique within the index set $\mathbb{N}$, such that for all $i \epsilon \mathbb{N}$ and for our fixed $K > 0$ and $k > n$ that we have

$$\left|\frac{p_i}{q_i} - x_0\right| < \frac{K}{q_i^k}$$

By $\left|\frac{p_i}{q_i} - x_0\right| < \frac{K}{q_i^k}$ we know that $\lim_{i \to \infty} \frac{p_i}{q_i} = x_0$. Pass to a subsequence $\left\{\frac{p_{i_j}}{q_{i_j}}\right\}_{j=1}^{\infty}$ and assume

$$\left\{\frac{p_{i_j}}{q_{i_j}}\right\}_{j=1}^{\infty} \epsilon \; (x_0 - 1, x_0 + 1), \forall \, j$$

and that each $\frac{p_{i_j}}{q_{i_j}}$ is closer to x_0 than to any other root of $f(x)$. So Proposition 13 holds.

Now we show $\left\{q_{i_j} \,\middle|\, j \epsilon \mathbb{N}\right\}$ is an unbounded set.

If the denominators $\left\{q_{i_j} \,\middle|\, j \epsilon \mathbb{N}\right\}$ are restricted to a bounded set (i.e., live within a finite interval, so there can only be a finite number of q_{i_j}) we get a contradiction: as the set S is infinite and each $\frac{p_{i_j}}{q_{i_j}}$ is unique within the set S, we have $\lim_{j \to \infty} p_{i_j} = \infty$ forced. As the q_{i_j} live in a bounded interval and $\lim_{j \to \infty} p_{i_j} = \infty$, after some finite point the inequality

$$\left|\frac{p_{i_j}}{q_{i_j}} - x_0\right| < \frac{K}{\left(q_{i_j}\right)^k}$$

must be proven false: as $\lim_{j \to \infty} p_{i_j} = \infty$, the term $\left|\frac{p_{i_j}}{q_{i_j}} - x_0\right| \to \infty$, but $K < \infty$ and $q_{i_j} \geq 1$, so $\frac{K}{\left(q_{i_j}\right)^k}$ is bounded, by K at most.

Thus $\lim_{j \to \infty} q_{i_j} = \infty$ is forced. And, an important inequality: by passing to a subsequence, we assume that for all i_j that

$$\left|\frac{p_{i_j}}{q_{i_j}} - x_0\right| \geq \frac{K}{\left(q_{i_j}\right)^k}$$

is true, for all i_j.

As $k > n$, we have $k - n \geq 1$. Now apply Proposition 13: On the interval $[x_0 - 1, x_0 + 1]$ by some $M > 0$ bound the absolute value of the derivative $\left|\frac{df}{dx}\right|$ of f. As x_0 is irrational, note the polynomial f is of degree at least 2; see Definition 3, so M is non-zero.

Now we derive our contradiction. Where M equals a bound of $\left|\frac{df}{dx}\right|$ in the range $[x_0 - 1, x_0 + 1]$, and remembering x_0 is an irrational root of our degree n polynomial $f(x) \epsilon \mathbb{Z}[x]$, and applying Proposition 13 we get:

$$\frac{K}{\left(q_{i_j}\right)^k} > \left|\frac{p_{i_j}}{q_{i_j}} - x_0\right| \geq \frac{1}{M \cdot \left(q_{i_j}\right)^n} > 0$$

Tossing the middle, and reversing the inequality,

$$\frac{1}{M \cdot \left(q_{i_j}\right)^n} < \frac{K}{\left(q_{i_j}\right)^k}$$

Doing algebra, the following is always true:

$$\left(q_{i_j}\right)^{k-n} < M \cdot K$$

But as $\lim_{j \to \infty} q_{i_j} = \infty$, and $k - n \geq 1$, for all but an at most finite set of j we have forced

$$q_{i_j}^{k-n} > M \cdot K$$

violating the inequality $\left(q_{i_j}\right)^{k-n} < M \cdot K$. Thus our initial assumption was wrong, and any set as in the proposition's statement is necessarily *finite* – this will be key to proving a number transcendental.

This verifies the proposition, and is our second "speed limit." □

Discussion 16

Putting together Proposition 13 and 15 with $K = 1$, let x_0 be an irrational algebraic number, and assume $f(x)$ the minimal polynomial of x_0, as the minimal polynomial gives the largest bound. Let $n = \deg(f)$. Fix $k = n + 1$, and M a bound as in Calculus Result 4.

In the next equation, for any sequence of unique rational numbers $\left\{\frac{p_i}{q_i}\right\}_{i=1}^{\infty}$ with $\lim_{i\to\infty}\frac{p_i}{q_i}=x_0$, whenever $\frac{p_i}{q_i}$ is "close" to x_0 (i.e., after some finite point), for a bound $M>0$ on the absolute value of the derivative of $f(x)$ on $[x_0-1, x_0+1]$ we have

$$\frac{1}{M\cdot q_i^n} \leq \left|\frac{p_i}{q_i} - x_0\right| \text{ (always true)}$$

For the next we have a best a finite set of q_i:

$$\left|\frac{p_i}{q_i} - x_0\right| < \frac{1}{q_i^k} \text{ (a finite set of } \frac{p_i}{q_i}\text{)}$$

Summarize: ignoring finite sets, in general for any rational sequence of unique rational numbers $\left\{\frac{p_i}{q_i}\right\}_{i=1}^{\infty}$ with $\lim_{i\to\infty}\frac{p_i}{q_i}=x_0$, whenever $\frac{p_i}{q_i}$ is "close" to x_0 (i.e., after some finite point i_0, for all $i \geq i_0$), for the above bound $M>0$ and $k>n$ we have two "speed limits,"

$$\left|\frac{p_i}{q_i} - x_0\right| \geq \frac{1}{M\cdot q_i^n} \text{ (always true)}$$

and,

$$\left|\frac{p_i}{q_i} - x_0\right| < \frac{K}{q_i^k} \text{—only true for a finite subset of } \left\{\frac{p_i}{q_i}\right\}_{i=1}^{\infty},$$

$$\text{so we can pass to a subsequence } \left\{\frac{p_{i_j}}{q_{i_j}}\right\}_{j=1}^{\infty} \text{ to make it never true}$$

The second of these facts is extremely important in Theorem 18, where we prove a number transcendental.

Now we create a transcendental number, i.e., a number x_1 such that x_1 is not the root of any polynomial with $f(x) \in \mathbb{Z}[x]$.

Definition 17

We define a new number x_1 in a special way. For now assume it an algebraic number, that is, the root of a minimal polynomial $f(x) \in \mathbb{Z}[x]$ of some degree n, and, the number n will play a role. Let

$$x_1 = \sum_{m=1}^{\infty} 10^{-m!}$$

In the exponential we use factorial function, as in $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$.

Apply a standard calculus test, the ratio test:

In a "generic" series $\sum_{m=1}^{\infty} a_m$, we have $a_m = 10^{-m!}$. Apply the ratio test:

$$\left|\frac{a_{m+1}}{a_m}\right| = \frac{10^{-(m+1)!}}{10^{-m!}} =$$

$$\frac{10^{m!}}{10^{(m+1)!}} = \frac{10^{m!}}{10^{(m+1)\cdot m!}} =$$

$$\frac{10^{m!}}{(10^{m!})^{m+1}}$$

It is easy that this converges to zero as $m \to \infty$, so the conditions of the root test are satisfied. We have $x_1 = \sum_{m=1}^{\infty} 10^{-m!}$ is an absolutely convergent series, so, is convergent.

The number x_1 is easily an infinite sum of rational numbers, and at each point i we define a term of an infinite sequence of rational numbers $\left\{\frac{p_i}{q_i}\right\}_{i=1}^{\infty}$ as

$$\frac{p_i}{q_i} = \sum_{m=1}^{i} 10^{-m!} = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \cdots + \frac{1}{10^{(i-1)!}} + \frac{1}{10^{i!}}$$

Algebra, to get a common denominator:

$$\frac{p_i}{q_i} = \frac{10^{i!-1!} + 10^{i!-2!} + 10^{i!-3!} \ldots + 10^{i!-(i-1)!} + 10^{i!-i!}}{10^{i}}$$

So as formulas, $q_i = \frac{1}{10^{i!}}$, and $p_i = \sum_{m=1}^{i} 10^{i!-m!}$. So,

$$\frac{p_i}{q_i} = \frac{10^{i!} + 10^{i!-1!} + 10^{i!-2!} + \cdots 10^{i!-(i-1)!} + 1}{10^{i!}} = \frac{\sum_{m=1}^{i} 10^{i!-m!}}{10^{i!}}$$

and this converges to x_1, so we have $\lim_{i\to\infty}\frac{p_i}{q_i}=x_1$.

We need to verify that Proposition 15 holds. It is easy to assign the denominator at each finite point i as $q_i = 10^{i!}$. And, it is easy that each q_i is unique. If $i \neq j$, note that

$$p_i = 10^{i!} + 10^{i!-1!} + 10^{i!-2!} + \cdots + 1$$

and

$$p_j = 10^{j!} + 10^{j!-1!} + 10^{j!-2!} + \cdots + 1$$

satisfy $p_i - p_j = \sum_{m=1}^{i} 10^{i!-m!} - \sum_{m=1}^{j} 10^{j!-m!}$, which as $i \neq j$ is non-zero—if $i > j$, it possesses $10^{i!-1!}$ which cannot cancel, and p_i and p_j are consequently different numbers. Also, for any m, note p_m always has a final digit of 1, so in $\frac{p_m}{q_m}$ no canceling is possible, as q_m equals a power of 10.

So, $\left\{\frac{p_i}{q_i}\right\}_{i=1}^{\infty}$ is a set of unique rational numbers, and Proposition 15 holds, that is, for any fixed $k > n$ and any fixed $K \in \mathbb{N}$, there exists an at most finite set S, indexed by some *finite* set $M = \{1, 2, 3 \ldots m\}$,

$$S = \left\{\frac{p_i}{q_i} \,\middle|\, i \in M; p_i, q_i \in \mathbb{Z}, q_i \neq 0\right\}$$

such that

$$\left|\frac{p_i}{q_i} - x_1\right| < \frac{K}{q_i^k}$$

Note x_1 is called the *Liouville Constant*, and $x_1 = 0.110001000000000000000001000\ldots$ with the 1's getting progressively farther and farther apart. As digits of x_1 never repeat, it is easily irrational. This means $\deg(f(x)) \geq 2$; see Definition 3.

Now we have some tools, our "big" theorem follows, and is to what we have been building up.

Theorem 18.

There does not exist a polynomial $f(x) \in \mathbb{Z}[x]$ of which x_1 is a root.

Proof.

*The **geometric constant π** is transcendental, but this was proven in 1882, over thirty years after Liouville's proof. This meant **squaring the circle** is impossible, solving a problem that had been open for thousands of years.*

Assume the contrary, i.e., that the number x_1 equals a root of some minimal polynomial $f(x) \epsilon \mathbb{Z}[x]$, and $f(x)$ is of some (possibly re-defined) degree $n \epsilon \mathbb{N}$; the degree n matters, and we will refer to it. The proof assumes n a known number, but this proof works, for any finite $n \epsilon \mathbb{N}$. Remember, as x_1 is irrational, n must be at least 2; see Definition 3.

From Definition 17 we have a sequence of unique rational numbers $\left\{\frac{p_i}{q_i}\right\}_{i=1}^{\infty}$ with $\lim_{i\to\infty}\frac{p_i}{q_i} = x_1$.

Remember, the denominator at each finite point i is $q_i = 10^{i!}$.

First we draw a bound. Fix $k = n + 1$.

Go back to our definition of x_1. The next line requires small re-ordering, but that's easy, inside absolute value brackets. Note that at any finite point i that

$$\left|\frac{p_i}{q_i} - x_1\right| = \left|\sum_{m=1}^{i} 10^{-m!} - \sum_{m=1}^{\infty} 10^{-m!}\right| =$$

$$\sum_{m=i+1}^{\infty} 10^{-m!} = \frac{1}{10^{(i+1)!}} + \frac{1}{10^{(i+2)!}} + \cdots$$

Or, simpler,

$$\left|\frac{p_i}{q_i} - x_1\right| = \frac{1}{10^{(i+1)!}} + \frac{1}{10^{(i+2)!}} + \cdots \qquad \text{(Equation 1)}$$

Now draw bounds: First let $i = k + 1 = n + 2$. As in Definition 17 we pointed out that the degree of $f(x)$ equals at least 2, we must have $i \geq 4$; see Definition 3; this will be mentioned, later. Thus as $k = i - 1$

$$(i + 1) \cdot i! = (i + 1)! >$$

$$(i - 1) \cdot i! = k \cdot i!$$

In short, $(i + 1)! > k \cdot i!$, and just as $3 > 2$ leads to $\frac{1}{3} < \frac{1}{2}$, we derive

$$\frac{1}{10^{(i+1)!}} < \frac{1}{10^{k \cdot i!}}$$

So, referring back to Equation (1) above, and adding some parentheses,

$$\left| \frac{p_i}{q_i} - x_1 \right| < \frac{1}{10^{k \cdot i!}} + \left(\frac{1}{10^{(i+2)!}} + \frac{1}{10^{(i+3)!}} + \cdots \right) \qquad \text{(Equation 2)}$$

For our fixed i and k, for some K we may easily write the right side as

$$\frac{K}{10^{k \cdot i!}} = \frac{1}{10^{k \cdot i!}} + \left(\frac{1}{10^{(i+2)!}} + \frac{1}{10^{(i+3)!}} + \cdots \right) \qquad \text{(Equation 3)}$$

Finding K is solving $\frac{K}{a} = \frac{1}{a} + b$ for K, and

$$K = \left(10^{k \cdot i!}\right) \cdot \left(\frac{1}{10^{k \cdot i!}} + \frac{1}{10^{(i+2)!}} + \frac{1}{10^{(i+3)!}} + \cdots \right)$$

Or,

$$K = 1 + \frac{1}{10^{(i+2)! - k \cdot i!}} + \frac{1}{10^{(i+3)! - k \cdot i!}} + \cdots \qquad \text{(Equation 4)}$$

On last, note that for $j \geq 2$, the number $10^{(i+j)! - k \cdot i!}$ is a positive power of ten: As we have here fixed $i = n + 2$, and as $n \geq 2$, we have $i \geq 4$; see Definition 3. As

- $i + 2 = n + 4$, and
- $i + 2 > k = n + 1$

we have $(i + j)! - k \cdot i!$ is an increasingly "large" exponent, and the right-side terms of Equation 4 get small, extremely fast. As an example, if $n = 2$, we have $i = 4, k = 3$, and set out a few exponents m on $\frac{1}{10^m}$:

1. $i = 4$ $\quad (i + 2)! - k \cdot i! = 6! - 3 \cdot 4! = 720 - 72 = 648$
2. $i = 5$ $\quad (i + 2)! - k \cdot i! = 7! - 3 \cdot 5! = 5040 - 360 = 4680$
3. $i = 6$ $\quad (i + 2)! - k \cdot i! = 8! - 3 \cdot 6! = 40320 - 2160 = 38160$

Also note n is known, so $i = k + 1 = n + 2$ are known, and K equals a value that can be determined. As the inequality is strict, it is easy to be a bit sloppy.

For $i = k + 2$ and larger values of i, the term

$$\frac{1}{10^{(i+3)!-k\cdot i!}}+\frac{1}{10^{(i+4)!-k\cdot i!}}+\cdots$$

only gets smaller. So in the bound, the same value of K will work, regardless of how big i is.

So combining Equations 2 and 3, we draw an important bound, for all $i \geq k+1$:

$$\left|\frac{p_i}{q_i}-x_1\right| = \sum_{m=i+1}^{\infty} 10^{-n!} < \frac{K}{10^{k\cdot i!}}$$

Or, simpler,

$$\left|\frac{p_i}{q_i}-x_1\right| < \frac{K}{10^{k\cdot i!}}$$

Note $\left\{\frac{p_i}{q_i}\right\}_{i=k}^{\infty}$ is an infinite sequence of unique rational numbers, and remember, $q_i = \frac{1}{10^{i!}}, \forall\, i$. For each $i > k > n$:

$$\left|\frac{p_i}{q_i}-x_1\right| < \frac{K}{10^{k\cdot i!}} =$$

$$\frac{K}{(10^{i!})^k} = \frac{K}{q_i^k}$$

In short,

$$\left|\frac{p_i}{q_i}-x_1\right| < \frac{K}{q_i^k}, \forall\, i > k$$

But this is true for all $i > k = n+1$, and $\left\{\frac{p_i}{q_i}\right\}_{i=k+1}^{\infty}$ is an infinite set, a direct contradiction to Proposition 15 and impossible if x_1 is an algebraic number. Thus x_1 is not an algebraic number.□

Final conclusion 13

By Theorem 12 the number $x_1 = \sum_{n=1}^{\infty} 10^{-n!}$ cannot be the root of any polynomial with coefficients in $\mathbb{Z}$ (equivalent, $\mathbb{Q}$), hence x_1 is not an algebraic number. That is to say, x_1 equals a transcendental number. □

Final comment 14

Again, just in the world of real numbers, as Cantor proved

- the algebraic numbers are *countable*, of cardinality $\aleph_0$ and
- the reals are *uncountable*, of cardinality $2^{\aleph_0}$,

it follows that transcendental numbers must be an uncountable set, that is, of cardinality $2^{\aleph_0}$. For such a large set, as of June 2017 precious few numbers have been *proven* transcendental.