Abel–Ruffini theorem

From Wikipedia, the free encyclopedia

In algebra, the **Abel–Ruffini theorem** (also known as **Abel's impossibility theorem**) states that there is no *general* algebraic solution—that is, solution in radicals— to polynomial equations of degree five or higher.[1] The theorem is named after Paolo Ruffini, who made an incomplete proof in 1799, and Niels Henrik Abel, who provided a proof in 1823. Évariste Galois independently proved the theorem in a work that was posthumously published in 1846.[2]

Contents

Interpretation

The content of this theorem is frequently misunderstood. It does *not* assert that higher-degree polynomial equations are unsolvable. In fact, the opposite is true: *every* non-constant polynomial equation in one unknown, with real or complex coefficients, has at least one complex number as solution; this is the fundamental theorem of algebra. Although the solutions cannot always be expressed exactly with radicals, they can be computed to any desired degree of accuracy using numerical methods such as the Newton–Raphson method or Laguerre method, and in this way they are no different from solutions to polynomial equations of the second, third, or fourth degrees.

The theorem only concerns the *form* that such a solution must take. The theorem says that *not all* solutions of higher-degree equations can be obtained by starting with the equation's coefficients and rational constants, and repeatedly forming sums, differences, products, quotients, and radicals (*n*-th roots, for some integer *n*) of previously obtained numbers. This clearly excludes the possibility of having any formula that expresses the solutions of an *arbitrary* equation of degree 5 or higher in terms of its coefficients, using only those operations, or even of having different formulas for different roots or for different classes of polynomials, in such a way as to cover all cases. (In principle one could imagine formulas using irrational numbers as constants, but even if a finite number of those were admitted at the start, not all roots of higher-degree equations could be obtained.) However some polynomial equations, of arbitrarily high degree, are solvable with such operations. Indeed, if the roots happen to be rational numbers, they can trivially be expressed as constants. The simplest nontrivial example is the equation $x^n = a$, where a is a positive real number, which has n solutions, given by:

$$x = \sqrt[n]{a} \cdot e^{i2\pi k/n}, \quad k = 0, 1, \ldots, n-1.$$

Here the expression $e^{i2\pi k/n}$, which appears to involve the use of the exponential function, in fact just gives the different possible values of $\sqrt[n]{1}$ (the *n*-th roots of unity), so it involves only extraction of radicals.

Lower-degree polynomials

The solutions of any second-degree polynomial equation can be expressed in terms of addition, subtraction, multiplication, division, and square roots, using the familiar quadratic formula: The roots of the following equation are shown below:

$$ax^2 + bx + c = 0, a \neq 0$$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Analogous formulas for third- and fourth-degree equations, using cube roots and fourth roots, had been known since the 16th century.

Quintics and higher

The Abel–Ruffini theorem says that there are *some* fifth-degree equations whose solution cannot be so expressed. The equation $x^5 - x + 1 = 0$ is an example. (See Bring radical.) Some other fifth degree equations *can* be solved by radicals, for example $x^5 - x^4 - x + 1 = 0$, which factorizes to $(x-1)(x-1)(x+1)(x+i)(x-i) = 0$. The precise criterion that distinguishes between those equations that can be solved by radicals and those that cannot was given by Évariste Galois and is now part of Galois theory: a polynomial equation can be solved by radicals if and only if its Galois group (over the rational numbers, or more generally over the base field of admitted constants) is a solvable group.

Today, in the modern algebraic context, we say that second, third and fourth degree polynomial equations can always be solved by radicals because the symmetric groups S_2, S_3 and S_4 are solvable groups, whereas S_n is not solvable for $n \geq 5$. This is so because for a polynomial of degree *n* with indeterminate coefficients (i.e., given by symbolic parameters), the Galois group is the full symmetric group S_n (this is what is called the "general equation of the *n*-th degree"). This remains true if the coefficients are concrete but algebraically independent values over the base field.

Proof

The following proof is based on Galois theory. Historically, Ruffini and Abel's proofs precede Galois theory.

One of the fundamental theorems of Galois theory states that an equation is solvable in radicals if and only if it has a solvable Galois group, so the proof of the Abel–Ruffini theorem comes down to computing the Galois group of the general polynomial of the fifth degree.

Let y_1 be a real number transcendental over the field of rational numbers Q, and let y_2 be a real number transcendental over $Q(y_1)$, and so on to y_5 which is transcendental over $Q(y_1, y_2, y_3, y_4)$. These numbers are called independent transcendental elements over Q. Let $E = Q(y_1, y_2, y_3, y_4, y_5)$ and let

$$f(x) = (x - y_1)(x - y_2)(x - y_3)(x - y_4)(x - y_5) \in E[x].$$

Multiplying $f(x)$ out yields the elementary symmetric functions of the y_n:

$$\begin{aligned}
s_1 &= y_1 + y_2 + y_3 + y_4 + y_5 \\
s_2 &= y_1y_2 + y_1y_3 + y_1y_4 + y_1y_5 + y_2y_3 + y_2y_4 + y_2y_5 + y_3y_4 + y_3y_5 + y_4y_5 \\
s_3 &= y_1y_2y_3+y_1y_2y_4+y_1y_2y_5+y_1y_3y_4+y_1y_3y_5+y_1y_4y_5+y_2y_3y_4+y_2y_3y_5+y_2y_4y_5+y_3y_4y_5 \\
s_4 &= y_1y_2y_3y_4 + y_1y_2y_3y_5 + y_1y_2y_4y_5 + y_1y_3y_4y_5 + y_2y_3y_4y_5 \\
s_5 &= y_1y_2y_3y_4y_5.
\end{aligned}$$

The coefficient of x^n in $f(x)$ is thus $(-1)^{5-n}s_{5-n}$. Because our independent transcendentals y_n act as indeterminates over Q, every permutation σ in the symmetric group on 5 letters S_5 induces an automorphism σ' on E that leaves Q fixed and permutes the elements y_n. Since an arbitrary rearrangement of the roots of the product form still produces the same polynomial, e.g.:

$$(y - y_3)(y - y_1)(y - y_2)(y - y_5)(y - y_4)$$

is still the same polynomial as

$$(y-y_1)(y-y_2)(y-y_3)(y-y_4)(y-y_5)$$

the automorphisms σ' also leave E fixed, so they are elements of the Galois group $G(E/Q)$. Now, since $|S_5| = 5!$ it must be that $|G(E/Q)| \geq 5!$, as there could possibly be automorphisms there that are not in S_5. However, since the relative automorphisms Q for splitting field of a quintic polynomial has at most 5! elements, $|G(E/Q)| = 5!$, and so $G(E/Q)$ must be isomorphic to S_5. Generalizing this argument shows that the Galois group of every general polynomial of degree n is isomorphic to S_n.

And what of S_5? The only composition series of S_5 is $S_5 \geq A_5 \geq \{e\}$ (where A_5 is the alternating group on five letters, also known as the icosahedral group). However, the quotient group $A_5/\{e\}$ (isomorphic to A_5 itself) is not an abelian group, and so S_5 is not solvable, so it must be that the general polynomial of the fifth degree has no solution in radicals. Since the first nontrivial normal subgroup of the symmetric group on n letters is always the alternating group on n letters, and since the alternating groups on n letters for $n \geq 5$ are always simple and non-abelian, and hence not solvable, it also says that the general polynomials of all degrees higher than the fifth also have no solution in radicals.

Note that the above construction of the Galois group for a fifth degree polynomial only applies to the *general polynomial*, specific polynomials of the fifth degree may have different Galois groups with quite different properties, e.g. $x^5 - 1$ has a splitting field generated by a primitive 5th root of unity, and hence its Galois group is abelian and the equation itself solvable by radicals. However, since the result is on the general polynomial, it does say that a general "quintic formula" for the roots of a quintic using only a finite combination of the arithmetic operations and radicals in terms of the coefficients is impossible. Q.E.D.

History

Around 1770, Joseph Louis Lagrange began the groundwork that unified the many different tricks that had been used up to that point to solve equations, relating them to the theory of groups of permutations, in the form of Lagrange resolvents. This innovative work by Lagrange was a precursor to Galois theory, and its failure to develop solutions for equations of fifth and higher degrees hinted that such solutions might be impossible, but it did not provide conclusive proof. The theorem, however, was first nearly proved by Paolo Ruffini in 1799, but his proof was mostly ignored. He had several times tried to send it to different mathematicians to get it acknowledged, amongst them, French mathematician Augustin-Louis Cauchy, but it was never acknowledged, possibly because the proof was spanning 500 pages. The proof also, as was discovered later, contained an error. Ruffini assumed that a solution would necessarily be a function of the radicals (in modern terms, he failed to prove that the splitting field is one of the fields in the tower of radicals which corresponds to a solution expressed in radicals). While Cauchy felt that the assumption was minor, most historians believe that the proof was not complete until Abel proved this assumption. The theorem is thus generally credited to Niels Henrik Abel, who published a proof that required just six pages in 1824.[3]

Insights into these issues were also gained using Galois theory pioneered by Évariste Galois. In 1885, John Stuart Glashan, George Paxton Young, and Carl Runge provided a proof using this theory.

In 1963, Vladimir Arnold discovered a topological proof of the Abel-Ruffini theorem,[4] which served as a starting point for topological Galois theory.[5]

See also

- Theory of equations

Notes

1. ^ Jacobson (2009), p. 211.
2. ^ Galois, Évariste (1846). "OEuvres mathématiques d'Évariste Galois." (http://visualiseur.bnf.fr/ark:/12148/cb343487840/date1846) . *Journal des mathématiques pures et appliquées* **XI**: 381–444. http://visualiseur.bnf.fr/ark:/12148/cb343487840/date1846. Retrieved 2009-02-04.

3. ^ du Sautoy, Marcus. "January: Impossibilities". *Symmetry: A Journey into the Patterns of Nature*. ISBN 978-0-06-078941-1.
4. ^ "Tribute to Vladimir Arnold" (http://www.ams.org/notices/201203/rtx120300378p.pdf) (PDF). *Notices of the American Mathematical Society* **59** (3): 393. March 2012. http://www.ams.org/notices/201203/rtx120300378p.pdf.
5. ^ "Vladimir Igorevich Arnold" (http://www.ams.org/distribution/mmj/vol10-3-2010/viarnold.html) . 2010. http://www.ams.org/distribution/mmj/vol10-3-2010/viarnold.html.

References

- Edgar Dehn. *Algebraic Equations: An Introduction to the Theories of Lagrange and Galois*. Columbia University Press, 1930. ISBN 0-486-43900-3.
- Jacobson, Nathan (2009), *Basic algebra*, **1** (2nd ed.), Dover, ISBN 978-0-486-47189-1
- John B. Fraleigh. *A First Course in Abstract Algebra*. Fifth Edition. Addison-Wesley, 1994. ISBN 0-201-59291-6.
- Ian Stewart. *Galois Theory*. Chapman and Hall, 1973. ISBN 0-412-10800-3.
- Abel's Impossibility Theorem at Everything2 (http://www.everything2.net/title/Abel%2527s+Impossibility+Theorem)

External links

- MÉMOIRE SUR LES ÉQUATIONS'ALGÉBRIQUES, OU L'ON DÉMONTRE. L'IMPOSSIBILITÉ DE LA RÉSOLUTION DE L'ÉQUATION GÉNÉRALE. DU CINQUIÈME DEGRÉ (http://www.abelprisen.no/verker/oeuvres_1881_del1/oeuvres_completes_de_abel_nouv_ed_1_kap03_opt.pdf) PDF - the first proof on 1824 in French
- Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré (http://www.abelprisen.no/verker/oeuvres_1839/oeuvres_completes_de_abel_1_kap02_opt.pdf) PDF - the second proof on 1826 in French

Retrieved from "http://en.wikipedia.org/w/index.php?title=Abel–Ruffini_theorem&oldid=520258984"

Categories: Solvable groups | Theorems in algebra | Galois theory | Polynomials | Niels Henrik Abel

- This page was last modified on 28 October 2012 at 13:04.
-

Fundamental theorem of algebra

From Wikipedia, the free encyclopedia

The **fundamental theorem of algebra** states that every non-constant single-variable polynomial with complex coefficients has at least one complex root. This includes polynomials with real coefficients, since every real number is a complex number with zero imaginary part.

Equivalently (by definition), the theorem states that the field of complex numbers is algebraically closed.

The theorem is also stated as follows: every non-zero, single-variable, degree *n* polynomial with complex coefficients has, counted with multiplicity, exactly *n* roots. The equivalence of the two statements can be proven through the use of successive polynomial division.

In spite of its name, there is no purely algebraic proof of the theorem, since any proof must use the completeness of the reals (or some other equivalent formulation of completeness), which is not an algebraic concept. Additionally, it is not fundamental for modern algebra; its name was given at a time when the study of algebra was mainly concerned with the solutions of polynomial equations with real or complex coefficients.

Contents

History

Peter Rothe (Petrus Roth), in his book *Arithmetica Philosophica* (published in 1608), wrote that a polynomial equation of degree *n* (with real coefficients) *may* have *n* solutions. Albert Girard, in his book *L'invention nouvelle en l'Algèbre* (published in 1629), asserted that a polynomial equation of degree *n* has *n* solutions, but he did not state that they had to be real numbers. Furthermore, he added that his assertion holds “unless the equation is incomplete”, by which he meant that no coefficient is equal to 0. However, when he explains in detail what he means, it is clear that he actually believes that his assertion is always true; for instance, he shows that the equation $x^4 = 4x - 3$, although incomplete, has four solutions (counting multiplicities): 1 (twice), $-1 + i\sqrt{2}$, and $-1 - i\sqrt{2}$.

As will be mentioned again below, it follows from the fundamental theorem of algebra that every non-constant polynomial with real coefficients can be written as a product of polynomials with real coefficients whose degree is either 1 or 2. However, in 1702 Leibniz said that no polynomial of the type $x^4 + a^4$ (with *a* real and distinct from 0) can be written in such a way. Later, Nikolaus Bernoulli made the same assertion concerning the polynomial $x^4 - 4x^3 + 2x^2 + 4x + 4$, but he got a letter from Euler in 1742[1] in which he was told that his polynomial happened to be equal to

$$(x^2 - (2+\alpha)x + 1 + \sqrt{7} + \alpha)(x^2 - (2-\alpha)x + 1 + \sqrt{7} - \alpha),$$

where α is the square root of $4 + 2\sqrt{7}$. Also, Euler mentioned that

$$x^4 + a^4 = (x^2 + a\sqrt{2} \cdot x + a^2)(x^2 - a\sqrt{2} \cdot x + a^2).$$

A first attempt at proving the theorem was made by d'Alembert in 1746, but his proof was incomplete. Among other problems, it assumed implicitly a theorem (now known as Puiseux's theorem) which would not be proved until more than a century later, and furthermore the proof assumed the fundamental theorem of algebra. Other attempts were made by Euler (1749), de Foncenex (1759), Lagrange (1772), and Laplace (1795). These last four attempts assumed implicitly Girard's assertion; to be more precise, the existence of solutions was assumed and all that remained to be proved was that their form was $a + bi$ for some real numbers a and b. In modern terms, Euler, de Foncenex, Lagrange, and Laplace were assuming the existence of a splitting field of the polynomial $p(z)$.

At the end of the 18th century, two new proofs were published which did not assume the existence of roots. One of them, due to James Wood and mainly algebraic, was published in 1798 and it was totally ignored. Wood's proof had an algebraic gap.[2] The other one was published by Gauss in 1799 and it was mainly geometric, but it had a topological gap, filled by Alexander Ostrowski in 1920, as discussed in Smale 1981 [3] (http://projecteuclid.org/DPubS?service=UI&version=1.0&verb=Display&handle=euclid.bams/1183547848) (Smale writes, "...I wish to point out what an immense gap Gauss' proof contained. It is a subtle point even today that a real algebraic plane curve cannot enter a disk without leaving. In fact even though Gauss redid this proof 50 years later, the gap remained. It was not until 1920 that Gauss' proof was completed. In the reference Gauss, A. Ostrowski has a paper which does this and gives an excellent discussion of the problem as well..."). A rigorous proof was published by Argand in 1806; it was here that, for the first time, the fundamental theorem of algebra was stated for polynomials with complex coefficients, rather than just real coefficients. Gauss produced two other proofs in 1816 and another version of his original proof in 1849.

The first textbook containing a proof of the theorem was Cauchy's *Cours d'analyse de l'École Royale Polytechnique* (1821). It contained Argand's proof, although Argand is not credited for it.

None of the proofs mentioned so far is constructive. It was Weierstrass who raised for the first time, in the middle of the 19th century, the problem of finding a constructive proof of the fundamental theorem of algebra. He presented his solution, that amounts in modern terms to a combination of the Durand–Kerner method with the homotopy continuation principle, in 1891. Another proof of this kind was obtained by Hellmuth Kneser in 1940 and simplified by his son Martin Kneser in 1981.

Without using countable choice, it is not possible to constructively prove the fundamental theorem of algebra for complex numbers based on the Dedekind real numbers (which are not constructively equivalent to the Cauchy real numbers without countable choice[3]). However, Fred Richman proved a reformulated version of the theorem that does work.[4]

Proofs

All proofs below involve some analysis, or at least the topological concept of continuity of real or complex functions. Some also use differentiable or even analytic functions. This fact has led some to remark that the Fundamental Theorem of Algebra is neither fundamental, nor a theorem of algebra.

Some proofs of the theorem only prove that any non-constant polynomial with real coefficients has some complex root. This is enough to establish the theorem in the general case because, given a non-constant polynomial $p(z)$ with complex coefficients, the polynomial

$$q(z) = p(z)\overline{p(\overline{z})}$$

has only real coefficients and, if z is a zero of $q(z)$, then either z or its conjugate is a root of $p(z)$.

A large number of non-algebraic proofs of the theorem use the fact (sometimes called “growth lemma”) that an n-th degree polynomial function $p(z)$ whose dominant coefficient is 1 behaves like z^n when $|z|$ is large enough. A more precise statement is: there is some positive real number R such that:

$$\tfrac{1}{2}|z^n| < |p(z)| < \tfrac{3}{2}|z^n|$$

when $|z| > R$.

Complex-analytic proofs

Find a closed disk D of radius r centered at the origin such that $|p(z)| > |p(0)|$ whenever $|z| \geq r$. The minimum of $|p(z)|$ on D, which must exist since D is compact, is therefore achieved at some point z_0 in the interior of D, but not at any point of its boundary. The minimum modulus principle implies then that $p(z_0) = 0$. In other words, z_0 is a zero of $p(z)$.

A variation of this proof that does not require the use of the minimum modulus principle (most proofs of which in turn require the use of Cauchy's integral theorem or some of its consequences) is based on the observation that for the special case of a polynomial function, the minimum modulus principle can be proved directly using elementary arguments. More precisely, if we assume by contradiction that $a := p(z_0) \neq 0$, then, expanding $p(z)$ in powers of $z - z_0$ we can write

$$p(z) = a + c_k(z - z_0)^k + c_{k+1}(z - z_0)^{k+1} + \ldots + c_n(z - z_0)^n.$$

Here, the c_j's are simply the coefficients of the polynomial $z \longrightarrow p(z + z_0)$, and we let k be the index of the first coefficient following the constant term that is non-zero. But now we see that for z sufficiently close to z_0 this has behavior asymptotically similar to the simpler polynomial $q(z) = a + c_k(z - z_0)^k$, in the sense that (as is easy to check) the function $\left|\frac{p(z) - q(z)}{(z - z_0)^{k+1}}\right|$ is bounded by some positive constant M in some neighborhood of z_0. Therefore if we define $\theta_0 = (\arg(a) + \pi - \arg(c_k))/k$ and let $z = z_0 + re^{i\theta_0}$, then for any sufficiently small positive number r (so that the bound M mentioned above holds), using the triangle inequality we see that

$$\begin{aligned} |p(z)| &< |q(z)| + r^{k+1}\left|\frac{p(z) - q(z)}{r^{k+1}}\right| \\ &\leq \left|a + (-1)c_k r^k e^{i(\arg(a) - \arg(c_k))}\right| + Mr^{k+1} \\ &= |a| - |c_k|r^k + Mr^{k+1}. \end{aligned}$$

When r is sufficiently close to 0 this upper bound for $|p(z)|$ is strictly smaller than $|a|$, in contradiction to the definition of z_0. (Geometrically, we have found an explicit direction θ_0 such that if one approaches z_0 from that direction one can obtain values $p(z)$ smaller in absolute value than $|p(z_0)|$.)

Another analytic proof can be obtained along this line of thought observing that, since $|p(z)| > |p(0)|$ outside D, the minimum of $|p(z)|$ on the whole complex plane is achieved at z_0. If $|p(z_0)| > 0$, then $1/p$ is a bounded holomorphic function in the entire complex plane since, for each complex number z, $|1/p(z)| \leq |1/p(z_0)|$. Applying Liouville's theorem, which states that a bounded entire function must be constant, this would imply that $1/p$ is constant and therefore that p is constant. This gives a contradiction, and hence $p(z_0) = 0$.

Yet another analytic proof uses the argument principle. Let R be a positive real number large enough so that every root of $p(z)$ has absolute value smaller than R; such a number must exist because every non-constant polynomial function of degree n has at most n zeros. For each $r > R$, consider the number

$$\frac{1}{2\pi i}\int_{c(r)} \frac{p'(z)}{p(z)}\,dz,$$

where $c(r)$ is the circle centered at 0 with radius r oriented counterclockwise; then the argument principle says that this number is the number N of zeros of $p(z)$ in the open ball centered at 0 with radius r, which, since $r > R$, is the total number of zeros of $p(z)$. On the other hand, the integral of n/z along $c(r)$ divided by $2\pi i$ is equal to n. But the difference between the two numbers is

$$\frac{1}{2\pi i}\int_{c(r)}\left(\frac{p'(z)}{p(z)} - \frac{n}{z}\right)dz = \frac{1}{2\pi i}\int_{c(r)} \frac{zp'(z) - np(z)}{zp(z)}\,dz.$$

The numerator of the rational expression being integrated has degree at most $n - 1$ and the degree of the denominator is $n + 1$. Therefore, the number above tends to 0 as r tends to $+\infty$. But the number is also equal to $N - n$ and so $N = n$.

Still another complex-analytic proof can be given by combining linear algebra with the Cauchy theorem. To establish that every complex polynomial of degree $n > 0$ has a zero, it suffices to show that every complex square matrix of size $n > 0$ has a (complex) eigenvalue.[5] The proof of the latter statement is by contradiction.

Let A be a complex square matrix of size $n > 0$ and let I_n be the unit matrix of the same size. Assume A has no eigenvalues. Consider the resolvent function

$$R(z) = (zI_n - A)^{-1},$$

which is a meromorphic function on the complex plane with values in the vector space of matrices. The eigenvalues of A are precisely the poles of $R(z)$. Since, by assumption, A has no eigenvalues, the function $R(z)$ is an entire function and Cauchy theorem implies that

$$\int_{c(r)} R(z)dz = 0.$$

On the other hand, $R(z)$ expanded as a geometric series gives:

$$R(z) = z^{-1}(I_n - z^{-1}A)^{-1} = z^{-1}\sum_{k=0}^{\infty}\frac{1}{z^k}A^k.$$

This formula is valid outside the closed disc of radius $||A||$ (the operator norm of A). Let $r > ||A||$. Then

$$\int_{c(r)} R(z)dz = \sum_{k=0}^{\infty}\int_{c(r)}\frac{dz}{z^{k+1}}A^k = 2\pi i I_n$$

(in which only the summand $k = 0$ has a nonzero integral). This is a contradiction, and so A has an eigenvalue.

Topological proofs

Let $z_0 \in \mathbf{C}$ be such that the minimum of $|p(z)|$ on the whole complex plane is achieved at z_0; it was seen at the proof which uses Liouville's theorem that such a number must exist. We can write $p(z)$ as a polynomial in $z - z_0$: there is some natural number k and there are some complex numbers $c_k, c_{k+1}, ..., c_n$ such that $c_k \neq 0$ and that

$$p(z) = p(z_0) + c_k(z - z_0)^k + c_{k+1}(z - z_0)^{k+1} + \cdots + c_n(z - z_0)^n.$$

It follows that if a is a k^{th} root of $-p(z_0)/c_k$ and if t is positive and sufficiently small, then $|p(z_0 + ta)| < |p(z_0)|$, which is impossible, since $|p(z_0)|$ is the minimum of $|p|$ on D.

For another topological proof by contradiction, suppose that $p(z)$ has no zeros. Choose a large positive number R such that, for $|z| = R$, the leading term z^n of $p(z)$ dominates all other terms combined; in other words, such that $|z|^n > |a_{n-1}z^{n-1} + \cdots + a_0|$. As z traverses the circle given by the equation $|z| = R$ once counter-clockwise, $p(z)$, like z^n, winds n times counter-clockwise around 0. At the other extreme, with $|z| = 0$, the “curve” $p(z)$ is simply the single (nonzero) point $p(0)$, whose winding number is clearly 0. If the loop followed by z is continuously deformed between these extremes, the path of $p(z)$ also deforms continuously. We can explicitly write such a deformation as $H(Re^{i\theta}, t) = p((1-t)Re^{i\theta})$ where t is greater than or equal to 0 and less than or equal to 1. If one views the variable t as time, then at time zero the curve is $p(z)$ and at time one the curve is $p(0)$. Clearly at every point t, $p(z)$ cannot be zero by the original assumption, therefore during the deformation, the curve never crosses zero. Therefore the winding number of the curve around zero should never change. However, given that the winding number started as n and ended as 0, this is absurd. Therefore, $p(z)$ has at least one zero.

Algebraic proofs

These proofs use two facts about real numbers that require only a small amount of analysis (more precisely, the intermediate value theorem):

- every polynomial with odd degree and real coefficients has some real root;
- every non-negative real number has a square root.

The second fact, together with the quadratic formula, implies the theorem for real quadratic polynomials. In other words, algebraic proofs of the fundamental theorem actually show that if *R* is any real-closed field, then its extension $C=R(\sqrt{-1})$ is algebraically closed.

As mentioned above, it suffices to check the statement “every non-constant polynomial *p*(*z*) with real coefficients has a complex root”. This statement can be proved by induction on the greatest non-negative integer *k* such that 2^k divides the degree *n* of *p*(*z*). Let *a* be the coefficient of z^n in *p*(*z*) and let *F* be a splitting field of *p*(*z*) over *C*; in other words, the field *F* contains *C* and there are elements $z_1, z_2, ..., z_n$ in *F* such that

$$p(z)=a(z-z_1)(z-z_2)\cdots(z-z_n).$$

If *k* = 0, then *n* is odd, and therefore *p*(*z*) has a real root. Now, suppose that $n = 2^k m$ (with *m* odd and *k* > 0) and that the theorem is already proved when the degree of the polynomial has the form $2^{k-1}m'$ with *m′* odd. For a real number *t*, define:

$$q_t(z)=\prod_{1\le i<j\le n}\left(z-z_i-z_j-tz_iz_j\right).$$

Then the coefficients of $q_t(z)$ are symmetric polynomials in the z_i's with real coefficients. Therefore, they can be expressed as polynomials with real coefficients in the elementary symmetric polynomials, that is, in $-a_1, a_2, ..., (-1)^n a_n$. So $q_t(z)$ has in fact *real* coefficients. Furthermore, the degree of $q_t(z)$ is $n(n-1)/2 = 2^{k-1}m(n-1)$, and $m(n-1)$ is an odd number. So, using the induction hypothesis, q_t has at least one complex root; in other words, $z_i + z_j + tz_iz_j$ is complex for two distinct elements *i* and *j* from {1,...,*n*}. Since there are more real numbers than pairs (*i*,*j*), one can find distinct real numbers *t* and *s* such that $z_i + z_j + tz_iz_j$ and $z_i + z_j + sz_iz_j$ are complex (for the same *i* and *j*). So, both $z_i + z_j$ and z_iz_j are complex numbers. It is easy to check that every complex number has a complex square root, thus every complex polynomial of degree 2 has a complex root by the quadratic formula. It follows that z_i and z_j are complex numbers, since they are roots of the quadratic polynomial $z^2 - (z_i + z_j)z + z_iz_j$.

J. Shipman showed in 2007 that the assumption that odd degree polynomials have roots is stronger than necessary; any field in which polynomials of prime degree have roots is algebraically closed (so "odd" can be replaced by "odd prime" and furthermore this holds for fields of all characteristics). For axiomatization of algebraically closed fields, this is the best possible, as there are counterexamples if a single prime is excluded. However, these counterexamples rely on −1 having a square root. If we take a field where −1 has no square root, and every polynomial of degree $n \in I$ has a root, where *I* is any fixed infinite set of odd numbers, then every polynomial *f*(*x*) of odd degree has a root (since $(x^2 + 1)^k f(x)$ has a root, where *k* is chosen so that $\deg(f) + 2k \in I$).

Another algebraic proof of the fundamental theorem can be given using Galois theory. It suffices to show that **C** has no proper finite field extension.[6] Let *K*/**C** be a finite extension. Since the normal closure of *K* over **R** still has a finite degree over **C** (or **R**), we may assume without loss of generality that *K* is a normal extension of **R** (hence it is a Galois extension, as every algebraic extension of a field of characteristic 0 is separable). Let *G* be the Galois group of this extension, and let *H* be a Sylow 2-group of *G*, so that the order of *H* is a power of 2, and the index of *H* in *G* is odd. By the fundamental theorem of Galois theory, there exists a subextension *L* of *K*/**R** such that Gal(*K*/*L*) = *H*. As [*L*:**R**] = [*G*:*H*] is odd, and there are no nonlinear irreducible real polynomials of odd degree, we must have *L* = **R**, thus [*K*:**R**] and [*K*:**C**] are powers of 2. Assuming for contradiction [*K*:**C**] > 1, the 2-group Gal(*K*/**C**) contains a subgroup of index 2, thus there exists a subextension *M* of **C** of degree 2. However, **C** has no extension of degree 2, because every quadratic complex polynomial has a complex root, as mentioned above.

Geometric proof

There exists still another way to approach the fundamental theorem of algebra, due to J. M. Almira and A. Romero: by Riemannian Geometric arguments. The main idea here is to prove that the existence of a non-constant polynomial *p*(*z*) without zeroes implies the existence of a flat Riemannian metric over the sphere S^2. This leads to a contradiction, since the sphere is not flat.

Recall that a Riemannian surface (*M*,*g*) is said to be flat if its Gaussian curvature, which we denote by K_g, is identically null. Now, Gauss-Bonnet theorem, when applied to the sphere S^2, claims that

$$\int_{S^2} K_g = 4\pi,$$

which proves that the sphere is not flat.

Let us now assume that $n > 0$ and $p(z) = a_0 + a_1z + \cdots + a_nz^n \neq 0$ for each complex number z. Let us define $p^*(z) = z^np(1/z) = a_0z^n + a_1z^{z-1} + \cdots + a_n$. Obviously, $p^*(z) \neq 0$ for all z in **C** . Consider the polynomial $f(z) = p(z)p^*(z)$. Then $f(z) \neq 0$ for each z in **C**. Furthermore,

$$f(1/w) = p(1/w)p^*(1/w) = (1/w)^{2n}p^*(w)p(w) = (1/w)^{2n}f(w).$$

We can use this functional equation to prove that g, given by

$$g = \frac{1}{|f(w)|^{\frac{2}{n}}}\,|dw|^2$$

for w in **C**, and

$$g = \frac{1}{|f(1/w)|^{\frac{2}{n}}}\,|d(1/w)|^2$$

for $w \in S^2\backslash\{0\}$, is a well defined Riemannian metric over the sphere S^2 (which we identify with the extended complex plane $\mathbf{C} \cup \{\infty\}$).

Now, a simple computation shows that

$$(\forall w \in \mathbb{C}) : \frac{1}{|f(w)|^{\frac{1}{n}}}\,K_g = \frac{1}{n}\Delta \log|f(w)| = \frac{1}{n}\Delta\,\mathbf{Re}\log f(w) = 0,$$

since the real part of an analytic function is harmonic. This proves that $K_g = 0$.

Corollaries

Since the fundamental theorem of algebra can be seen as the statement that the field of complex numbers is algebraically closed, it follows that any theorem concerning algebraically closed fields applies to the field of complex numbers. Here are a few more consequences of the theorem, which are either about the field of real numbers or about the relationship between the field of real numbers and the field of complex numbers:

- The field of complex numbers is the algebraic closure of the field of real numbers.
- Every polynomial in one variable x with real coefficients is the product of a constant, polynomials of the form $x + a$ with a real, and polynomials of the form $x^2 + ax + b$ with a and b real and $a^2 - 4b < 0$ (which is the same thing as saying that the polynomial $x^2 + ax + b$ has no real roots).
- Every rational function in one variable x, with real coefficients, can be written as the sum of a polynomial function with rational functions of the form $a/(x - b)^n$ (where n is a natural number, and a and b are real numbers), and rational functions of the form $(ax + b)/(x^2 + cx + d)^n$ (where n is a natural number, and a, b, c, and d are real numbers such that $c^2 - 4d < 0$). A corollary of this is that every rational function in one variable and real coefficients has an elementary primitive.
- Every algebraic extension of the real field is isomorphic either to the real field or to the complex field.

Bounds on the zeroes of a polynomial

Main article: Properties of polynomial roots

While the fundamental theorem of algebra states a general existence result, it is of some interest, both from the theoretical and from the practical point of view, to have information on the location of the zeroes of a given polynomial. The simpler result in this direction is a bound on the modulus: all zeroes ζ of a monic polynomial $z^n+a_{n-1}z^{n-1}+\cdots+a_1z+a_0$ satisfy an inequality $|\zeta|\leq R_\infty,$ where

$$R_\infty := 1+\max\{|a_0|,\cdots,|a_{n-1}|\}.$$

Notice that, as stated, this is not yet an existence result but rather an example of what is called an a priori bound: it says that *if there are solutions* then they lie inside the closed disk of center the origin and radius R_∞. However, once coupled with the fundamental theorem of algebra it says that the disk contains in fact at least one solution. More generally, a bound can be given directly in terms of any p-norm of the n-vector of coefficients $a:=(\ a_0,\ a_1,\ldots,\ a_{n-1})$, that is $|\zeta|\leq R_p$, where R_p is precisely the *q*-norm of the 2-vector $(1,\|a\|_p)$, *q* being the conjugate exponent of *p*, 1/*p* + 1/*q* = 1, for any $1\leq p\leq\infty$. Thus, the modulus of any solution is also bounded by

$$R_1 := \max\Big\{1, \sum_{0\leq k<n}|a_k|\Big\},$$
$$R_p := \Big[1+\Big(\sum_{0\leq k<n}|a_k|^p\Big)^{q/p}\Big]^{1/q},$$

for $1<p<\infty$, and in particular

$$R_2 := \sqrt{\sum_{0\leq k\leq n}|a_k|^2}$$

(where we define a_n to mean 1, which is reasonable since 1 is indeed the *n*-th coefficient of our polynomial). The case of a generic polynomial of degree n, $P(z):=a_nz^n+a_{n-1}z^{n-1}+\cdots+a_1z+a_0$, is of course reduced to the case of a monic, dividing all coefficients by $a_n\neq0$. Also, in case that 0 is not a root, i.e. $a_0\neq0$, bounds from below on the roots ζ follow immediately as bounds from above on $\frac{1}{\zeta}$, that is, the roots of $a_0z^n+a_1z^{n-1}+\cdots+a_{n-1}z+a_n$. Finally, the distance $|\zeta-\zeta_0|$ from the roots ζ to any point ζ_0 can be estimated from below and above, seeing $\zeta-\zeta_0$ as zeroes of the polynomial $P(z+\zeta_0)$, whose coefficients are the Taylor expansion of $P(z)$ at $z=\zeta_0$.

We report here the proof of the above bounds, which is short and elementary. Let ζ be a root of the polynomial $z^n+a_{n-1}z^{n-1}+\cdots+a_1z+a_0$; in order to prove the inequality $|\zeta|\leq R_p$ we can assume, of course, $|\zeta|>1$. Writing the equation as $-\zeta^n=a_{n-1}\zeta^{n-1}+\cdots+a_1\zeta+a_0$, and using the Hölder's inequality we find $|\zeta|^n\leq\|a\|_p\,\|(\zeta^{n-1},\cdots,\zeta,1)\|_q$. Now, if $p=1$, this is $|\zeta|^n\leq\|a\|_1\max\{|\zeta|^{n-1},\cdots,|\zeta|,1\}=\|a\|_1|\zeta|^{n-1}$, thus $|\zeta|\leq\max\{1,\|a\|_1\}$. In the case $1<p\leq\infty$, taking into account the summation formula for a geometric progression, we have

$$|\zeta|^n\leq\|a\|_p\left(|\zeta|^{q(n-1)}+\cdots+|\zeta|^q+1\right)^{1/q}=\|a\|_p\left(\frac{|\zeta|^{qn}-1}{|\zeta|^q-1}\right)^{1/q}\leq\|a\|_p\left(\frac{|\zeta|^{qn}}{|\zeta|^q-1}\right)^{1/q},$$

thus $|\zeta|^{nq}\leq\|a\|_p^q\frac{|\zeta|^{qn}}{|\zeta|^q-1}$ and simplifying, $|\zeta|^q\leq1+\|a\|_p^q$. Therefore $|\zeta|\leq\|(1,\|a\|_p)\|_q=R_p$ holds, for all $1\leq p\leq\infty.$

Notes

1. ^ See section *Le rôle d'Euler* in C. Gilain's article *Sur l'histoire du théorème fondamental de l'algèbre: théorie des équations et calcul intégral.*
2. ^ Concerning Wood's proof, see the article *A forgotten paper on the fundamental theorem of algebra*, by Frank Smithies.
3. ^ For the minimum necessary to prove their equivalence, see Bridges, Schuster, and Richman; 1998; A weak countable choice principle; available from [1] (http://www.math.fau.edu/richman/HTML/DOCS.HTM) .
4. ^ See Fred Richman; 1998; The fundamental theorem of algebra: a constructive development without choice; available from [2] (http://www.math.fau.edu/richman/HTML/DOCS.HTM) .
5. ^ A proof of the fact that this suffices can be seen here.
6. ^ A proof of the fact that this suffices can be seen here.

References

Historic sources

- Cauchy, Augustin Louis (1821), *Cours d'Analyse de l'École Royale Polytechnique, 1ère partie: Analyse Algébrique* (http://gallica.bnf.fr/ark:/12148/bpt6k29058v) , Paris: Éditions Jacques Gabay (published 1992), ISBN 2-87647-053-5, http://gallica.bnf.fr/ark:/12148/bpt6k29058v (tr. Course on Analysis of the Royal Polytechnic Academy, part 1: Algebraic Analysis)
- Euler, Leonhard (1751), "Recherches sur les racines imaginaires des équations" (http://bibliothek.bbaw.de/bbaw/bibliothek-digital/digitalequellen/schriften/anzeige/index_html?band=02-hist/1749&seite:int=228) , *Histoire de l'Académie Royale des Sciences et des Belles-Lettres de Berlin* (Berlin) **5**: 222–288, http://bibliothek.bbaw.de/bbaw/bibliothek-digital/digitalequellen/schriften/anzeige/index_html?band=02-hist/1749&seite:int=228. English translation: Euler, Leonhard (1751), "Investigations on the Imaginary Roots of Equations" (http://www.mathsym.org/euler/e170.pdf) (PDF), *Histoire de l'Académie Royale des Sciences et des Belles-Lettres de Berlin* (Berlin) **5**: 222–288, http://www.mathsym.org/euler/e170.pdf
- Gauss, Carl Friedrich (1799), *Demonstratio nova theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse*, Helmstedt: C. G. Fleckeisen (tr. New proof of the theorem that every integral rational algebraic function of one variable can be resolved into real factors of the first or second degree).
- C. F. Gauss, "Another new proof of the theorem that every integral rational algebraic function of one variable can be resolved into real factors of the first or second degree (http://www.paultaylor.eu/misc/gauss-web.php) ", 1815
- Kneser, Hellmuth (1940), "Der Fundamentalsatz der Algebra und der Intuitionismus" (http://www-gdz.sub.uni-goettingen.de/cgi-bin/digbib.cgi?PPN266833020_0046) , *Mathematische Zeitschrift* **46**: 287–302, doi:10.1007/BF01181442 (http://dx.doi.org/10.1007%2FBF01181442) , ISSN 0025-5874 (//www.worldcat.org/issn/0025-5874) , http://www-gdz.sub.uni-goettingen.de/cgi-bin/digbib.cgi?PPN266833020_0046 (The Fundamental Theorem of Algebra and Intuitionism).
- Kneser, Martin (1981), "Ergänzung zu einer Arbeit von Hellmuth Kneser über den Fundamentalsatz der Algebra" (http://www-gdz.sub.uni-goettingen.de/cgi-bin/digbib.cgi?PPN266833020_0177) , *Mathematische Zeitschrift* **177** (2): 285–287, doi:10.1007/BF01214206 (http://dx.doi.org/10.1007%2FBF01214206) , ISSN 0025-5874 (//www.worldcat.org/issn/0025-5874) , http://www-gdz.sub.uni-goettingen.de/cgi-bin/digbib.cgi?PPN266833020_0177 (tr. An extension of a work of Hellmuth Kneser on the Fundamental Theorem of Algebra).
- Ostrowski, Alexander (1920), "Über den ersten und vierten Gaußschen Beweis des Fundamental-Satzes der Algebra" (http://gdz.sub.uni-goettingen.de/dms/load/img/?PPN=PPN236019856&DMDID=dmdlog53) , *Carl Friedrich Gauss* Werke *Band X Abt. 2*, http://gdz.sub.uni-goettingen.de/dms/load/img/?PPN=PPN236019856&DMDID=dmdlog53 (tr. On the first and fourth Gaussian proofs of the Fundamental Theorem of Algebra).
- Weierstraß, Karl (1891). "Neuer Beweis des Satzes, dass jede ganze rationale Function einer Veränderlichen dargestellt werden kann als ein Product aus linearen Functionen derselben Veränderlichen". *Sitzungsberichte der königlich preussischen Akademie der Wissenschaften zu Berlin*. pp. 1085–1101. (tr. New proof of the theorem that every integral rational function of one variable can be represented as a product of linear functions of the same variable).

Recent literature

- Almira, J.M.; Romero, A. (2007), "Yet another application of the Gauss-Bonnet Theorem for the sphere" (http://projecteuclid.org/DPubS/Repository/1.0/Disseminate?handle=euclid.bbms/1179839226&view=body&content-type=pdf_1) , *Bull. Belg. Math. Soc. Simon Stevin* **14**: 341–342, http://projecteuclid.org/DPubS/Repository/1.0/Disseminate?handle=euclid.bbms/1179839226&view=body&content-type=pdf_1

- Almira, J.M.; Romero, A. (2012), "Some Riemannian geometric proofs of the Fundamental Theorem of Algebra" (http://www.mathem.pub.ro/dgds/v14/D14-al.pdf) , *Differential Geometry - Dynamical Systems* **14**: 1–4, http://www.mathem.pub.ro/dgds/v14/D14-al.pdf

- Fine, Benjamin; Rosenberger, Gerhard (1997), *The Fundamental Theorem of Algebra*, Undergraduate Texts in Mathematics, Berlin: Springer-Verlag, ISBN 978-0-387-94657-3
- Gersten, S.M.; Stallings, John R. (1988), "On Gauss's First Proof of the Fundamental Theorem of Algebra", *Proceedings of the AMS* **103** (1): 331–332, doi:10.2307/2047574 (http://dx.doi.org/10.2307%2F2047574) , ISSN 0002-9939 (//www.worldcat.org/issn/0002-9939) , JSTOR 2047574 (http://www.jstor.org/stable/2047574)
- Gilain, Christian (1991), "Sur l'histoire du théorème fondamental de l'algèbre: théorie des équations et calcul intégral", *Archive for History of Exact Sciences* **42** (2): 91–136, doi:10.1007/BF00496870 (http://dx.doi.org

/10.1007%2FBF00496870) , ISSN 0003-9519 (//www.worldcat.org/issn/0003-9519) (tr. On the history of the fundamental theorem of algebra: theory of equations and integral calculus.)

- Netto, Eugen; Le Vavasseur, Raymond (1916), "Les fonctions rationnelles §80–88: Le théorème fondamental", in Meyer, François; Molk, Jules, *Encyclopédie des Sciences Mathématiques Pures et Appliquées, tome I, vol. 2*, Éditions Jacques Gabay, 1992, ISBN 2-87647-101-9 (tr. The rational functions §80–88: the fundamental theorem).
- Remmert, Reinhold (1991), "The Fundamental Theorem of Algebra", in Ebbinghaus, Heinz-Dieter; Hermes, Hans; Hirzebruch, Friedrich, *Numbers*, Graduate Texts in Mathematics 123, Berlin: Springer-Verlag, ISBN 978-0-387-97497-2
- Shipman, Joseph (2007), "Improving the Fundamental Theorem of Algebra", *Mathematical Intelligencer* **29** (4): 9–14, doi:10.1007/BF02986170 (http://dx.doi.org/10.1007%2FBF02986170) , ISSN 0343-6993 (//www.worldcat.org/issn/0343-6993)
- Smale, Steve (1981), "The Fundamental Theorem of Algebra and Complexity Theory", *Bulletin (new series) of the American Mathematical Society* **4** (1) [4] (http://projecteuclid.org/DPubS?service=UI&version=1.0&verb=Display&handle=euclid.bams/1183547848)
- Smith, David Eugene (1959), *A Source Book in Mathematics*, Dover, ISBN 0-486-64690-4
- Smithies, Frank (2000), "A forgotten paper on the fundamental theorem of algebra", *Notes & Records of the Royal Society* **54** (3): 333–341, doi:10.1098/rsnr.2000.0116 (http://dx.doi.org/10.1098%2Frsnr.2000.0116) , ISSN 0035-9149 (//www.worldcat.org/issn/0035-9149)
- van der Waerden, Bartel Leendert (2003), *Algebra*, **I** (7th ed.), Springer-Verlag, ISBN 0-387-40624-7

External links

- Fundamental Theorem of Algebra (http://www.cut-the-knot.org/do_you_know/fundamental2.shtml) — a collection of proofs
- D. J. Velleman: *The Fundamental Theorem of Algebra: A Visual Approach*, PDF (unpublished paper) (http://www.cs.amherst.edu/~djv/) , visualisation of d'Alembert's, Gauss's and the winding number proofs
- Fundamental Theorem of Algebra Module by John H. Mathews (http://math.fullerton.edu/mathews/c2003/FunTheoremAlgebraMod.html)
- Bibliography for the Fundamental Theorem of Algebra (http://math.fullerton.edu/mathews/c2003/FunTheoremAlgebraBib/Links/FunTheoremAlgebraBib_lnk_2.html)
- *From the Fundamental Theorem of Algebra to Astrophysics: A "Harmonious" Path* (http://www.ams.org/notices/200806/tx080600666p.pdf)

Retrieved from "http://en.wikipedia.org/w/index.php?title=Fundamental_theorem_of_algebra&oldid=520436249"
Categories: Field theory | Theorems in algebra | Theorems in complex analysis | Fundamental theorems

- This page was last modified on 29 October 2012 at 15:05.
-