Modern Algebra Lecture Notes: Rings and fields set 11

Kevin Broughan

University of Waikato, Hamilton, New Zealand

May 22, 2010

Fundamental Theorem of Algebra

Comment

This has a fascinating history and many different proofs: see the Wikipedia article. The proof we will give is "algebraic".

Statement

Let $f(x) \in \mathbb{C}[x]$ be a non-constant polynomial. Then $f(x)$ factors completely in $\mathbb{C}$ as the product of linear factors: $f(x) = a(x - a_1)(\cdots)(x - a_n)$ where $a, a_i \in \mathbb{C}$.

Assumptions

(1) An complex number has a complex or real square root.

(2) Any polynomial with real coefficients and odd degree has a real root.

(3) Any polynomial with real coefficients has a splitting field.

(4) Any symmetric polynomial in n indeterminants over a field is a polynomial with coefficients in the field in the elementary symmetric polynomials. For example, with $n = 3$

$$a^3 + b^3 + c^3 = (a+b+c)^3 - 3(a+b+c)(ab+bc+ca) + 3abc = s_1^3 - 3s_1s_2 + 3s_3$$

where the s_i are the coefficients of $(x-a)(x-b)(x-c)$ when expanded.

Proof

(5) If $f(x) \in \mathbb{C}[x]$ then $g(x) = f(x)\overline{f(\bar{x})} \in \mathbb{R}[x]$. If $g(a) = 0$ for some $a \in \mathbb{C}$ then $f(a) = 0$ or $f(\bar{a}) = 0$. Hence we can assume $f(x) \in \mathbb{R}[x]$. We can also assume $f(x)$ is monic.

(6) We need only find **one** root for $f(x)$ in $\mathbb{C}$, since if every $f(x) \in \mathbb{C}[x]$ which is non-constant has a complex root, say $x = a$, then we can apply this result to $f(x)/(x-a)$ and get another root if the ratio is not constant, and so on.

(7) Let $n = \deg f(x) > 0$, $f(x) \in \mathbb{R}[x]$, and write $n = 2^k m$ where m is odd. If $k = 0$ then we can find a real, hence complex, root using assumption 2. above. Assume, to get a proof by induction, that the result is true for all polynomials of degree $2^e m$ with m odd and $e = 0, 1, 2, \ldots k$ and let $f(x)$ have degree $n = 2^{k+1} m$.

(8) So $f(x) \in \mathbb{R}[x]$ and is monic. By assumption (2) there is a field extension E of $\mathbb{R}$ in which $f(x)$ has a full set of roots, i.e. a splitting field for $f(x)$. In other words elements $a_1, \ldots, a_n$ in E such that $f(a_i) = 0$ and $f(x) = (x - a_1)(\cdots)(x - a_n)$.

The key definition

(9) Let $t \in \mathbb{R}$ and define

$$q_t(x) = \prod_{1 \leq i < j \leq n} (x - a_i - a_j - t a_i a_j).$$

The the coefficients of $q_t(x)$ are symmetric polynomials in the a_i with real coefficients, so the can be expressed as polynomials in the elementary symmetric polynomials with real coefficients. Since $f(x)$ has real coefficients each of these is in fact a real number, so $q_t(x)$ has real coefficients.

(10) The degree of $q_t(x)$ is $n(n-1)/2 = 2^k m(n-1)$ which a k'th power of 2 times an odd number, since n is even. Hence we can apply the inductive hypothesis and find a complex root a for $q_t(x)$. This means there are a pair of integers i, j such that $a = a_i + a_j + t a_i a_j \in \mathbb{C}$.

$$q_t(x) = \prod_{1 \le i < j \le n} (x - a_i - a_j - t a_i a_j).$$

(11) Now vary $t \in \mathbb{R}$ and for each such t find a pair i_t, j_t. Since there are only a finite number of possible pairs and an infinite number of $t's$ there must be at least one fixed pair i, j with an associated infinite number of $t's$.

(12) In particular a distinct t_1 and t_2 in $\mathbb{R}$ such that $a_i + a_j + t_1 a_i a_j \in \mathbb{C}$ and $a_i + a_j + t_2 a_i a_j \in \mathbb{C}$. This gives two linear equations in $\mathbb{C}$ for the unknowns $a_i + a_j$ and $a_i a_j$, which therefore must both be in $\mathbb{C}$.

(13) So $g(x) = x^2 - (a_i + a_j)x + a_i a_j \in \mathbb{C}[x]$, and using the quadratic formula, gives the roots $a_i, a_j \in \mathbb{C}$. But a_i is a root of the original polynomial $f(x)$ and we are done.$\square$

Algebraically closed

Definition

We say a field F is algebraically closed if every polynomial with coefficients in F splits completely in F. Then such a field F has no proper algebraic extensions $F(a)$. We have just shown that $\mathbb{C}$ is algebraically closed.

Algebraic closure

Given a field F, we say an extension E of F is an algebraic closure if E is algebraically closed and every polynomial with coefficients in F splits completely in E. Given F, its algebraic closure always exists and is unique up to isomorphism.

Example

The algebraic closure of $\mathbb{Q}$ is $\mathbb{A}$ the set of all algebraic numbers. This is not an easy fact to demonstrate. For example it means that the roots of

$$x^5 + \sqrt{3 + \sqrt{2 + \sqrt{5}}}x^4 - 4534^{\frac{1}{5}}x + i2^{\frac{1}{101}}$$

are algebraic numbers over $\mathbb{Q}$, i.e. satisfy a polynomial with rational coefficients (what might it be!).

Gelfond Schneider Theorem

It was a long worked on problem, celebrated by David Hilbert at the start of the 20th century, whether or not an algebraic number to an algebraic power was algebraic, for example $2^{\sqrt{2}}$. We must exclude some possibilities e.g. $(\sqrt{2})^2 = 2$. It was proved, by Gelfond and Schneider, in 1934 as follows:

Statement

If a and b are algebraic numbers with $a \neq 0$, and if b is not a rational number, then any value of $a^b = \exp(b \log a)$ for non-zero $\log a$ is a transcendental number.

Consequences

1. The number $2^{\sqrt{2}}$ is tanscendental.
2. $(1 + \sqrt{3})^{\sqrt{2}}$ is transcendental.
3. Both e and π cannot both be algebraic, since $e^{i\pi} = -1$.
4. Numbers of the form $e^{\frac{m}{n}}$, $m, n \in \mathbb{N}$ must be transcendental, since if not $e^{\frac{m}{n}} = a$ would be algebraic so $e^m = a^n$ would also be algebraic, $f(e^m) = 0$, $f(x) \in \mathbb{Q}[x]$. But if $g(x) := f(x^m)$ we would have $g(e) = 0$, so e would be algebraic, but it is not.

Unsolved problems

(1) Is $e + \pi$ transcendental ? It is not even known after hundreds of years whether or not it is irrational.

(2) If the Euler number

$$\gamma = \lim_{n\to\infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n\right)$$

irrational or rational ?

(3) We know

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}, \text{ and } \sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90},$$

and $\sum_{n=1}^{\infty} \frac{1}{n^3}$ is irrational, but is it a rational multiple of π^3, making it transcendental ?

(4) We know the multiplicative group $GF(p) := \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ is cyclic. Artin's conjecture is that for each $a \in \mathbb{N},\ a > 1$ there are an infinite number of primes p such that a generates $GF(p)$.