

On the Fundamental Theorem of Algebra

Harold M. Edwards
New York University

Everyone knows what is meant by the fundamental theorem of algebra: *The field of complex numbers is algebraically closed.* In other words, any polynomial with complex coefficients can be written as a product of linear factors with complex coefficients.

My goal in this half hour is to convince you that a different theorem deserves the name.

First, an historical argument:

In the 18th century, Euler, Lagrange, and Laplace attempted to prove that a polynomial of degree n has n complex roots. In 1799, the 22 year old Gauss presented a proof as his doctoral dissertation. He disparaged earlier proofs, saying that they *assumed* that the given polynomial could be written as a product of linear factors

$$\begin{aligned} f(x) &= a_0x^n + a_1x^{n-1} + \cdots + a_n \\ &= a_0 \prod_{i=1}^n (x - \rho_i) \end{aligned}$$

and were therefore circular arguments, because they provided no way of understanding what the roots might be if they were not complex numbers.

In 1815, Gauss published a second and altogether different proof. It is much closer to the proofs of Euler, Lagrange, and Laplace than it is to his own first proof. The argument is an induction on the number of times that 2 divides n . If n is odd, then of course the polynomial has a real root. If n is $2^i m$ where m is odd, he constructs an auxiliary polynomial whose degree is divisible just $i - 1$ times by 2 and proves that a complex root of the auxiliary polynomial implies a complex root of the original.

The construction of the auxiliary polynomial is very close to the 18th century proofs he had criticized so seriously before. The *idea* of the construction is that the coefficients of the auxiliary polynomial are symmetric polynomials in the roots and therefore can be expressed in terms of the coefficients of the polynomial itself, but of course the actual construction must circumvent this argument because the “roots” of the polynomial are not defined *a priori*.

Which brings me to my main point: This notion that it is valid to do computations *as if* a given polynomial had roots is in my opinion the truly fundamental theorem of algebra:

Given a polynomial $f(x)$, there is a field containing the coefficients of f over which f is a product of linear factors.

In short, a polynomial has a splitting field.

But this statement is still too vague to be called a theorem. Let me first give a few examples of the precise theorem I have in mind.

First example:

$$\begin{aligned} x^3 - 2 &\equiv \left(x - \frac{z^4}{18}\right) \left(x + \frac{z^4 - 18z}{36}\right) \left(x + \frac{z^4 + 18z}{36}\right) \\ &\quad \text{mod } (z^6 + 108) \end{aligned}$$

(Reason: $(\frac{z^4}{18})^3 \equiv \frac{z^{12}}{3^6 2^3} \equiv \frac{108^2}{3^6 2^3} \equiv 2$ and $(\frac{z^3}{6})^2 \equiv \frac{-108}{36} \equiv -3 \pmod{z^6 + 108}$, so $\frac{1}{2}(-1 + \frac{z^3}{6})$ is a cube root of unity mod $z^6 + 108$. Therefore, the presence of one cube root of 2 in the field $\mathbf{Q}[z] \pmod{z^6 + 108}$ implies two others.)

The formula says that if you ‘adjoin’ a sixth root of -108 you construct a field in which $x^3 - 2$ splits into linear factors. To say z is a sixth root of -108 means that you compute with it as a number but that you may replace z^6 with -108 whenever it is convenient to do so. This is what is meant by the field $\mathbf{Q}[z] \pmod{z^6 + 108}$. This is the ring of polynomials in z with rational coefficients, added and multiplied in the ordinary ways, when the relation $z^6 = -108$ is used. The fact that the polynomial $z^6 + 108$ is *irreducible* (a fact I will ask you to take my word for) implies that the ring defined in this way is in fact a field.

More generally,

$$x^3 - c \equiv (x - \frac{z^4}{9c})(x + \frac{z^4 - 9cz}{18c})(x + \frac{z^4 + 9cz}{18c}) \pmod{z^6 + 27c^2}$$

holds for *indeterminate* c .

Thus the field $\mathbf{Q}(c)[z] \pmod{z^6 + 27c^2}$ (here $\mathbf{Q}(c)$ denotes the field of rational functions in c with integer coefficients, a field over which the polynomial $z^6 + 27c^2$ is irreducible, so that polynomials in z with coefficients in that field modulo $z^6 + 27c^2$ is a field—the field that adjoins one root of $X^6 + 27c^2$ to $\mathbf{Q}(c)$. Again, the polynomial is irreducible, so the ring is a field.) The formula shows that this field is one over which $x^3 - c$ can be written as a product of linear factors. Somewhat more picturesquely: Adjoining one root of $z^6 + 27c^2$ gives three roots of $x^3 - c$.

A Fundamental Theorem of Algebra (Kronecker). *Let R be the ring $\mathbf{Z}[c_1, c_2, \dots, c_m]$ of polynomials in indeterminates c_1, c_2, \dots, c_m (m may be zero) with integer coefficients. Given a polynomial $f(x)$ with coefficients in R , there is an irreducible polynomial $g(z)$ with coefficients in R such that $f(x)$ factors mod $g(z)$ into a product of linear factors.*

In short, you can construct a splitting field of a given polynomial f in this specific way.

The auxiliary polynomial in Gauss’s second proof is $F(u, x) = \prod (u - (\rho_i + \rho_j)x + \rho_i \rho_j)$, where the product is over all pairs of integers (i, j) for which $1 \leq i < j \leq n$. The idea is that if the degree of f is divisible by 2 exactly ν times then the degree of F is divisible by 2 exactly $\nu - 1$ times; it is shown that if you pick any integer X for which $F(u, X)$ is relatively prime to its derivative with respect to u (a condition that is satisfied by all but a finite number of integers X) then a complex root of $F(u, X)$ implies a complex root of $f(x)$.

Note that our alternative fundamental theorem is what allows us to talk about the roots of f and of $F(u, X)$ and to compute with them. In particular, it makes sense of the definition of F . Gauss has to make sense of it in a more convoluted way.

I will sketch the gist of Gauss’s proof that a complex root of $F(u, X)$ implies a complex root of the original polynomial $f(x)$ in a moment.

Note first that it proves that any polynomial with integer coefficients has a complex root. If the degree is odd, this follows from the easy fact that a polynomial with integer

coefficients of odd degree has at least one *real* root. If the degree is twice an odd number, Gauss's construction gives an auxiliary polynomial of odd degree, one complex root of which implies a complex root of the original polynomial; since the auxiliary polynomial in fact has a real root, the original polynomial has a complex root. Then if the degree of the original polynomial is 4 times an odd number, Gauss's auxiliary polynomial has degree twice an odd number, therefore has a complex root, therefore the original polynomial has a complex root, and so forth. In short, every polynomial with integer coefficients has a complex root.

The main point is that the argument—given Gauss's assertion that a complex root of the auxiliary polynomial $F(u, X)$ implies a complex root of the polynomial itself—is entirely algebraic. The theorem being proved, involving complex numbers as it does, is *not* an algebraic theorem. One is required to construct a convergent sequence of numbers $a_j + ib_j$, in which the a_j and b_j are rational numbers, such that $f(a_j + ib_j) \rightarrow 0$. The inductive step shows that if you can do this for $F(u, X)$ for some integer X , then you can do it for $f(x)$.

Note that f is assumed to have *integer* coefficients, not complex ones.

(1) It is quite easy to prove that the truth of the statement that a polynomial with integer coefficients has *one* complex root implies that every polynomial whose coefficients are *algebraic numbers* can be written as a product of linear factors with complex coefficients.

(2) A polynomial whose coefficients are transcendental numbers is not an algebraic object and can't have anything to do with any fundamental theorem of algebra.

(3) The only reason polynomials with complex coefficients ever came into the picture was to go from the proof that there is *one* root to the proof that *all* roots are complex numbers. But our new fundamental theorem takes care of that: *All* roots of f are rationally expressible in terms of *one* root of a well-chosen g .

In short, careful reflection leads to the conclusion that the wrong theorem got the name.

Kronecker's 'fundamental theorem' has several advantages:

(A) Historically, it seems to be the natural first step in the proof of the theorem about complex roots.

(B) It is an algebraic theorem with an algebraic proof.

(C) It can be proved constructively.

(D) It serves as a natural basis for Galois theory, because it applies to polynomials whose coefficients are *letters* as well as numbers.

Here's the gist of Gauss's proof: With $F(u, x) = \prod(u - (\rho_i + \rho_j)x + \rho_i\rho_j)$, where the product is over all pairs of integers (i, j) for which $1 \leq i < j \leq n$, we have $F(u + w\frac{\partial F}{\partial x}, x - w\frac{\partial F}{\partial u}) = F(u, x)\phi(u, x, w)$ where ϕ is the polynomial in three variables with rational coefficients

$$\prod_{1 \leq i < j \leq n} \left(1 - w((\rho_i + \rho_j) \cdot \frac{\partial}{\partial x} \left(\frac{F(u, x)}{u - (\rho_i + \rho_j)x + \rho_i\rho_j} \right) - \rho_i\rho_j \cdot \frac{\partial}{\partial u} \left(\frac{F(u, x)}{u - (\rho_i + \rho_j)x + \rho_i\rho_j} \right)) \right)$$

(an easy computation). (Again, the vital role of Kronecker's theorem is that it makes sense of these algebraic computations with the roots of the original polynomial.) Choose an integer X for which $F(u, X)$ has distinct roots, i.e., this polynomial in u is relatively prime to its derivative. By the induction assumption, $F(u, X)$ has a complex root, call it U .

The values U' and X' of $\frac{\partial F}{\partial u}$ and $\frac{\partial F}{\partial x}$ at $(u, x) = (U, X)$ are then complex numbers. By the definition of ϕ ,

$$F(U + X'w, X - U'w) = F(U, X)\phi(U, X, w)$$

holds for variable w , and this complex number is zero by the choice of U . Define $x = X - U'w$ to find $F(U + X' \cdot \frac{X-x}{U'}, x) = 0$. (By the choice of X , $U' \neq 0$.) Setting $u = x^2$ in the definition of F gives $F(x^2, x) = \prod_{i,j} (x - \rho_i)(x - \rho_j)$, from which it follows that $F(x^2, x) = f(x)^{n-1}$. Thus, any solution x of the quadratic equation $x^2 = U + X' \cdot \frac{X-x}{U'}$ satisfies $f(x)^{n-1} = 0$, so it is a complex number on the one hand (the quadratic formula) and it is a root of f on the other.