The Fundamental Theorem of Algebra from a Constructive Point of View

(Slides of a talk given at Carnegie-Mellon University, April 15, 2004)

Fundamental Theorem of Algebra. *A polynomial of degree n has n roots.*

Some revisions. First,

Fundamental Theorem of Algebra. *A polynomial of degree n with integer coefficients has n roots.*

In order to deal with multiplicities, it is better to say, since α is a root of $f(x)$ if and only if $x - \alpha$ is a root of $f(x)$, that:

Fundamental Theorem of Algebra. *A polynomial with integer coefficients can be written as a product of linear factors*

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_n = a_0(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Since $f(x)$ can be written as a constant times a product of factors linear in x if and only if the same is true of the *monic* polynomial $a_0^{n-1}f(x/a_0) = x^n + a_1x^{n-1} + a_0a_2x^{n-2} + \cdots + a_0^{i-1}a_ix^{n-i} + \cdots + a_0^{n-1}a_n$, there is no loss of generality in assuming that the given polynomial is monic and stating the theorem in the form:

Fundamental Theorem of Algebra. *A monic polynomial with integer coefficients can be written as a product of monic linear factors.*

Stating the theorem in this simple form has the great virtue of showing that it is obviously false.

How, for example, could we factor $x^3 - 2$ into monic linear factors? You may say that the complex numbers contain three cube roots of 2 and the needed factors are $x - \alpha$ for these three complex numbers α.

In my opinion, resorting at this point to so sophisticated a notion as the complex numbers—which entail real numbers and limits and all the rest—is wholly premature.

The fundamental theorem was known—it was more or less an axiom—as early as the 17th century. One thinks of Girard and Newton, among others.

Many attempts were made to prove it in the 18th century—D'Alembert, Euler, Lagrange all wrote on the subject—but Gauss in 1799 in his doctoral dissertation rejected all their proofs as circular, saying that they used *computations in the roots* to prove that the roots were complex numbers, and that such computations could only be justified by first proving the theorem.

He published another proof in 1815 which more or less followed the lines of the proofs he had rejected in 1799. I like to think that at this time he came to the realization that the *real* theorem is the statement that:

Fundamental Theorem. *Given a monic polynomial with integer coefficients, there is a valid way to compute with its roots.*

I have come to believe that Euclid's practice of having two types of 'propositions'—'theorems' and 'constructions'—should be revived and 'constructions' should play a much larger role in our mathematics. The 'Fundamental Theorem' can be stated as a construction:

Given a monic polynomial with integer coefficients, construct a system of computation that extends rational computation with integers in such a way that it becomes possible to factor the given polynomial into monic linear factors.

To 'construct a system of computation' may sound like a formidable task, but it isn't at all. For example, it is easy to construct a system of computation in which $x^3 - 2$ has a monic linear factor:

The objects with which we will compute will be polynomials in an indeterminate y whose coefficients are rational numbers. They will be added and multiplied in the usual way. Two such polynomials will be considered to be *equal* if their difference is a multiple of $y^3 - 2$. Since constant polynomials are equal in this sense only if they are identical, this 'system' of computation includes within it ordinary computations with integers (and therefore ordinary computations with rational numbers).

Of course, we don't want to be too permissive in accepting something as a 'system of computation'. Rational computation requires addition, subtraction, multiplication and division. Aye, division, there's the rub.

Division by a quantity can be described as multiplication by its reciprocal, so what we want to know is that, in computations with polynomials in y of the type described, every quantity other than zero has a reciprocal.

Or, to use modern terminlogy, *the ring* $\mathbf{Q}[y] \bmod (y^3 - 2)$ *of polynomials in* y *with rational coefficients modulo* $y^3 - 2$ *is a field.*

This follows from the 'Euclidean algorithm' for polynomials, a simple construction that enables one to write the greatest common divisor of two nonzero polynomials as a linear combination of them (just as the actual Euclidean algorithm enables one to write the greatest common divisor of two integers as a sum of multiples of the integers).

Thus, if $h(y)$ is some polynomial in y that is not equal, mod y^3-2 to zero, then, *because* y^3-2 *is irreducible,* $h(y)$ and y^3-2 are relatively prime, so, by the Euclidean algorithm, there are polynomials $r(y)$ and $s(y)$ for which

$$r(y)h(y) + s(y)(y^3 - 2) = 1.$$

Then $r(y)$ is the reciprocal of $h(y)$ in the ring $\mathbf{Q}[y]$ mod (y^3-2), which is therefore a field.

In a similar way, given an irreducible monic polynomial $g(y)$ with integer coefficients, the ring $\mathbf{Q}[y] \bmod g(y)$ is a field. I'll call it the field **obtained by adjoining a root of $g(y)$ to the field of rational numbers**, because these computations simply *declare* that $g(y) = 0$ and base all computations on that declaration.

When we regard $x^3 - 2$ as a polynomial with coefficients in the field $\mathbf{Q}[y] \bmod (y^3 - 2)$ it has a linear factor—it has a root in this field—explicitly

$$x^3 - 2 \equiv x^3 - y^3 \equiv (x - y)(x^2 + xy + y^2) \bmod (y^3 - 2).$$

But one root isn't good enough. We want three.

Recap: Given a monic, irreducible polynomial $g(y)$ with integer coefficients, the field obtained by adjoining one root of g to the field $\mathbf{Q}$ of rational numbers is by definition the field $\mathbf{Q}[y]$ mod $g(y)$. It may well contain only *one* root of g, though, and we want $\deg g$ roots.

Let me pause a moment to remark how easy it is compute in the field $\mathbf{Q}[y]$ mod $g(y)$ when $g(y)$ is monic. In this case, $g(y) = y^m + b_1 y^{m-1} + b_2 y^{n-2} + \cdots + b_m$. Each element of the field is represented by one and only one polynomial in y, with rational coefficients, whose degree is less than m. Elements are added in the obvious way, and multiplied by multiplying the polynomials and then using $y^m = -b_1 y^{m-1} - \cdots - b_m$ to reduce the degree.

Fundamental Theorem (perhaps one should call it the Fundamental Construction). *Given a monic polynomial $f(x)$ with integer coefficients, construct an irreducible monic polynomial $g(y)$ with the property that adjunction of one root of $g(y)$ to* $\mathbf{Q}$ *gives a field over which $f(x)$ factors into linear factors.*

In my abstract I mentioned Galois. In fact, Galois gave a construction of such a $g(y)$, which is often called a **Galois resolvent**. But there is a catch. Galois's 'construction' *used* computations with the roots, so it can't be used to *justify* computations with the roots.

But it certainly gives a simple, concrete way to 'extend computations in $\mathbf{Q}$' in a way that factors $f(x)$.

The classic example is that $f(x) = x^3 - 2$ *can be factored into linear factors if you adjoin a single root* y *of* $y^6 + 108$. The specific formula is:

$$x^3 - 2 \equiv (x - \frac{y^4}{18})(x + \frac{y^4 - 18y}{36})(x + \frac{y^4 + 18y}{36}) \mod (y^6 + 108).$$

Indeed, one cube root of 2 comes from $(\frac{y^4}{18})^3 = \frac{(-108)^2}{18^3} = \frac{6 \cdot 6}{18} = 2$. To find two others, it is necessary and sufficient to find two primitive cube roots of 1.

But the primitive cube roots of 1 are $\frac{-1 \pm \sqrt{-3}}{2}$, so all we need is a square root of -3, which is provided by $(\frac{y^3}{6})^2 = \frac{-108}{36} = -3$, whereupon the proof of the formula becomes a simple exercise.

The name ‘Fundamental Theorem of Algebra’ is too firmly settled on the statement that a polynomial of degree n has n complex roots (counted with multiplicities) to expect it to change, but in my opinion the theorem I just stated is much more fundamental.

And it is a theorem of *algebra,* which the other is not.

Kronecker in 1887 stated a generalization of the factorization of $x^3 - 2$, namely,

$$\begin{aligned} & x^3 - c \\ & \quad \equiv (x - \frac{y^4}{9c})(x + \frac{y^4 - 9cy}{18c})(x + \frac{y^4 + 9cy}{18c}) \\ & \quad \mod (y^6 + 27c^2). \end{aligned}$$

Here both $f(x)$ and $g(y)$ have coefficients not in the ring of integers but in the ring $\mathbf{Z}[c]$ of polynomials in one indeterminate c with integer coefficients.

This is a very natural generalization of the fundamental theorem I have been talking about, that has no counterpart in the case of the 'Fundamental Theorem of Algebra'.

Note that the roots $\frac{y^4}{9c}$, $\frac{-y^4+9cy}{18c}$, $\frac{-y^4-9cy}{18c}$ are in the field obtained by adjoining one root y of $y^6 + 27c^2$ to the field of rational functions in c.

Fundamental Theorem (Construction). *Given a monic polynomial $f(x)$ with coefficients in the ring $\mathbf{Z}[c_1, c_2, \ldots, c_\nu]$ (polynomials in $c_1, c_2, \ldots, c_\nu$ with integer coefficients), construct a monic irreducible polynomial $g(y)$ with coefficients in the same ring such that adjunction of one root of g to the field of rational functions in $c_1, c_2, \ldots, c_\nu$ gives a field over which $f(x)$ factors into linear factors.*

(The field of rational functions in $c_1, c_2, \ldots, c_\nu$ is simply the field of quotients of the integral domain $\mathbf{Z}[c_1, c_2, \ldots, c_\nu]$.)

This theorem can be proved—by which I mean, of course, that the construction can be carried out—by very specific, finite algorithms.

I don't have time to describe them here. I will say that the key element, which took me years to find, is an algorithm that factors $f(x)$ mod $g(y)$ when f and g are monic irreducible polynomials with integer coefficients, or, more generally, with coefficients in $\mathbf{Z}[c_1, c_2, \ldots, c_\nu]$.

Note that this is no problem at all if you take a nonconstructive view of it. Then you can just say: Keep factoring as long as any of the factors you have can be factored further.

From a constructive point of view, even factorization over $\mathbf{Q}$ requires more than this, not to mention factorization over $\mathbf{Q}[y]$ mod $g(y)$.

One reason I consider the theorem I have stated more important than the usual fundamental theorem of algebra is that it *implies* that theorem in a very simple way:

It says that *all* roots of a given $f(x)$ can be expressed *rationally* in terms of *one* root of $g(y)$. Once you have done this you have expressions of *all* roots of $f(x)$ as complex numbers once you have an expression of *one* root of $g(y)$ as a complex number.

But to find *one* complex root of a given polynomial with integer coefficients is a fairly easy calculus problem. Essentially all you have to do is find a good approximation to a root and then set up an iteration that will find it to more and more decimal places.

Another way to state what I have been saying is that:

(1) Given any monic $f(x)$ with coefficients in $\mathbf{Z}[c_1, c_2, \ldots, c_\nu]$, you can construct a splitting field for it by adjoining to the field of rational functions in $c_1, c_2, \ldots, c_\nu$ a single root of a suitable monic irreducible $g(y)$, with coefficients in the same ring, that can be constructed.

(2) When $\nu = 0$, so that the coefficient ring is the ring of integers, this splitting field can be described as a subfield of the field of complex numbers simply by finding one complex root of $g(y)$.

In my opinion, it is an outright *mistake,* however, to regard the splitting field as a subfield of the complex numbers. Complex numbers are limits and can only be described by infinite sequences of approximations. They are always in a state of becoming, not of being. An element of a splitting field, on the other hand, is a root of a polynomial equation and as such can be described exactly in the sense that one can write down a finite set of rules to make it possible to compute it to any prescribed degree of accuracy.

Kronecker took a position that seems extreme in our times—he rejected the notion of a general infinite sequence and insisted that mathematics should only deal with sequences that could be generated by finite algorithms.

Now that I have come to see the fundamental theorem of algebra in the way I have described, I no longer regard this as such an outlandish idea. In fact, it presents a very worthwhile challenge:

Develop mathematical subjects in ways that conform to Kronecker's principles.

It's not as hard to do as you might imagine, and it directs your thoughts in invigorating ways.

The title of my forthcoming book is 'Essays in Constructive Mathematics'.