2.5 The Fundamental Theorem of Algebra.

We've seen formulas for the (complex) roots of quadratic, cubic and quartic polynomials. It is then reasonable to ask: "Do all the polynomials with rational (or complex) coefficients have complex roots?", and if this is true, then: "Are there formulas for the roots of polynomials in all degrees?"

The Fundamental Theorem of Algebra: All polynomials in $\mathbb{C}[x]$ (other than the constants) have complex roots.

So the answer to the first question is "yes." But the answer to the second question, mysteriously, is "no:"

Abel's Theorem: There is no formula that will always produce the complex roots of a polynomial of degree ≥ 5.

So there are no general formulas. But the word "always" in the statement of the theorem is important. Obviously **some** polynomials, like $x^n - 2$, **do** have roots that are given by a formula. This makes the following refinement, due to Galois, extremely interesting.

Galois' Theorem: There is a "group of symmetries" attached to each prime polynomial in $\mathbb{Q}[x]$ that explains whether of not there is a formula for its roots.

These are some serious theorems, and they are not easy to prove.
(We will not even attempt the theorems of Abel and Galois until later.)

The simplest proof of the Fundamental Theorem uses analysis. Here it is:

Proof of the Fundamental Theorem of Algebra: Given $f(x) \in \mathbb{C}[x]$, let $f(z)$ be the same polynomial thought of as a **function** of the (complex) variable z.

The graph of:

$$f(z) : \mathbb{C} \to \mathbb{C}$$

is hard to visualize, since it lives in $\mathbb{C}^2 = \mathbb{R}^4$, so instead we'll work with:

$$|f(z)| : \mathbb{C} \to \mathbb{R}$$

which we **can** visualize, as its graph lives in $\mathbb{R}^3$. We will write $z = s + ti$ and $|f(z)| = u$, so that the coordinates on $\mathbb{R}^3$ are (s, t, u).

Examples: (a) If $f(x) = a$ is a constant polynomial, the graph of the function $|f(z)| = |a|$ is the horizontal plane $u = |a|$.

(b) If $f(x) = x$, then $|f(z)| = |z| = \sqrt{s^2 + t^2}$, so:

$$u^2 = s^2 + t^2$$

is the graph of $|z|$. This is a cone with vertex at the origin.

More generally, the graph of $|z - z_0|$ is a cone with vertex at $(z_0, 0)$ (z_0 is a complex number!). These cones are good examples of graphs of functions that are continuous, but not differentiable (at the vertex).

(c) If $f(x) = x^2$, then $|f(z)| = |(s+ti)|^2 = s^2 + t^2$, so the graph is:

$$u = s^2 + t^2$$

which is a paraboloid meeting the *st*-plane at the origin.

On the other hand, the graph of

$$|z^2 - 1| = |z-1| \cdot |z+1|$$

is not a translated paraboloid. It has two points of intersection with the *st*-plane, namely the points $(1,0,0)$ and $(-1,0,0)$, and very near these points, the graph looks like a cone. Thus this function, too, is not differentiable at these two points.

Back to the Proof: The function $|f(z)|$ is continuous everywhere. If $f(x)$ has a root α, then $|f(\alpha)| = 0$ is a (global) minimum for the function $|f(z)|$, since the absolute value is non-negative. Thus proving that there are roots of $f(x)$ is the same thing as proving that $|f(z)|$ has global minimum equal to 0. We will prove that such minima occur, if the polynomial is not a constant. Let's write:

$$f(x) = a_d x^d + a_{d-1}x^{d-1} + ... + a_0$$

Then the proof follows from:

A couple of analytic observations:

(a) If $f(x)$ is not constant, then on **circles** $C \subset \mathbb{C}$ centered at 0 of big enough radius,

$$|f(z)| > |f(0)| \text{ for all } z \in C$$

We'll prove this below. But first recall that the **disc** D consisting of C together with all the interior points of C is **compact**, and that the continuous function:

$$|f(z)| : D \to \mathbb{R}$$

must therefore have maximum and minimum values somewhere in D. The maxima can (and do) live on C, which is the boundary of D, without being local maxima of $|f(z)|$, but for any C satisfying (a), we know that:

$$|f(0)| < |f(z)| \text{ for all points } z \in C$$

so all global minima must be in the **interior** of D, and therefore they must also be **local** minima of the function $|f(z)|$. But I claim:

(b) All the local minima of $|f(z)|$ satisfy $|f(\alpha)| = 0$.

Putting these together, (a) says there **must** be minima in the interior of big enough circles, and (b) says that each minimum value of the function is 0, so each $\alpha \in \mathbb{C}$ that realizes the minimum must satisfy $|f(\alpha)| = 0$. That is, α is a root!

So we have to prove (a) and (b). The key is to think about limits. These are "large" limits: the behavior of $f(z)$ for large values of $|z|$, and "small" limits: the behavior of $f(z)$ very close to a fixed $z_0 \in \mathbb{C}$.

Large Limits: $f(z) = a_d z^d + ... + a_0$ "grows like" $a_d z^d$ for large z.

Small Limits: $f(z)$ has Taylor expansions (Exercise 7-1):

$$f(z) = f(z_0) + b_1(z - z_0) + ... + b_d(z - z_0)^d$$

where

$$b_k = \frac{f^{(k)}(z_0)}{k!}$$

and then $f(z)$ "looks like" $f(z_0) + b_k(z - z_0)^k$ when z is close to z_0, and $f^{(k)}(z_0)$ is the first non-zero derivative.

To make all this precise, we need the **triangle inequality:**

$$|z + w| \le |z| + |w| \quad \text{or (setting } v = z + w) \quad |v| \le |v - w| + |w|$$

which it is convenient to rewrite as:

$$|w| \ge |v| - |v - w| = |v| - |w - v|$$

Proof of (a): By the triangle inequality:

$$|f(z)| \ge |a_d z^d| - |f(z) - a_d z^d| = |a_d|R^d - |a_{d-1}z^{d-1} + ... + a_0|$$

and also by the triangle inequality:

$$|a_{d-1}z^{d-1} + ... + a_0| \le |a_{d-1}z^{d-1}| + ... + |a_0|$$

so putting this all together, we get:

$$|f(z)| \ge |a_d|R^d - |a_{d-1}|R^{d-1} - ... - |a_0|$$

whenever $|z| = R$. i.e. z is on the circle of radius R centered at 0. We conclude from this that when R is very large, $|f(z)|$ grows like $|a_d|R^d$, and so can be made as large as we please. But let's be very precise about this. Take $R > 1$ and also:

$$R > \frac{|a_{d-1}| + ... + |a_0| + |f(0)|}{|a_d|}$$

Then:

$$\begin{aligned}
|a_d|R^d &= (|a_d|R)R^{d-1} \\
&> (|a_{d-1}| + ... + |a_0| + |f(0)|)R^{d-1} \\
&= |a_{d-1}|R^{d-1} + |a_{d-2}|R^{d-1} + ... + |a_0|R^{d-1} + |f(0)|R^{d-1} \\
&> |a_{d-1}|R^{d-1} + |a_{d-2}|R^{d-2} + ... + |a_0| + |f(0)|
\end{aligned}$$

(becuase we made sure that $R > 1$) so

$$|f(z)| \geq |a_d|R^d - |a_{d-1}|R^{d-1} - ... - |a_0| > |f(0)|$$

when $|z| = R$.

Example: Consider the polynomial

$$f(x) = 3x^4 + 2x - 1$$

In this case $|f(0)| = 1$, and the proof above tells us that if:

$$R > \frac{2+1+1}{3} = \frac{4}{3}$$

then $|f(z)| > 1$ whenever $|z| = R > 4/3$. In particular, notice that this tells us that any roots of $f(x)$ must be inside the disc of radius $4/3$! Exercise 9-1 gives an even better estimate.

Proof of (b): Let b_k be a complex number other than zero, and consider the function (of the variable z):

$$|f(z_0) + b_k(z - z_0)^k|$$

We can solve $b_k(z - z_0)^k = w$ for **any** complex number w by taking

$$z = \sqrt[k]{\frac{w}{b_k}} + z_0$$

(for any of the kth roots of w/b_k) so if $f(z_0) \neq 0$, we can be very clever and choose $w = -rf(z_0)$ for some real number $r < 1$ and solve:

$$z = \sqrt[k]{\frac{-rf(z_0)}{b_k}} + z_0$$

to conclude that:

$$|f(z_0) + b_k(z - z_0)^k| = |f(z_0) - rf(z_0)| = (1 - r)|f(z_0)| < |f(z_0)|$$

In other words, we've shown that if $|f(z_0)| > 0$, then z_0 is **not** a minimum of the function:

$$|f(z_0) + b_k(z - z_0)^k|$$

Now we turn to the function we're really interested in:

$$|f(z)| = |f(z_0) + b_k(z - z_0)^k + ... + b_d(z - z_0)^d|$$

(the Taylor series of $f(z)$, where I've deleted all the zero coefficients). The idea is that if we make $|z - z_0|$ small enough, and r small enough, then we come to the same conclusion: z_0 is not a local minimum because there are nearby values of z with smaller values of $|f(z)|$!

Precisely, we will choose r satisfying:

$$\sqrt[k]{\frac{r|f(z_0)|}{|b_k|}} < \frac{|b_k|}{|b_{k+1}| + ... + |b_d|}$$

or, in other words:

$$r < \left(\frac{|b_k|}{|b_{k+1}| + ... + |b_d|}\right)^k \frac{|b_k|}{|f(z_0)|}$$

and as in the previous page, we solve:

$$z = \sqrt[k]{\frac{-rf(z_0)}{b_k}} + z_0$$

and conclude that:

$$|z - z_0| = \left|\sqrt[k]{\frac{-rf(z_0)}{b_k}}\right| < \frac{|b_k|}{|b_{k+1}| + ... + |b_d|}$$

and we will additionally choose the r small enough to guarantee that $|z-z_0| < 1$. Now we use the triangle inequality and our inequalities:

$$\begin{aligned}
|f(z)| &\leq |f(z_0) + b_k(z - z_0)^k| + |b_{k+1}||z - z_0|^{k+1} + ... + |b_d||z - z_0|^d \\
&= (1 - r)|f(z_0)| + |z - z_0|^{k+1}\left(|b_{k+1}| + ... + |b_d||z - z_0|^{d-k-1}\right) \\
&< (1 - r)|f(z_0)| + |z - z_0|^{k+1}\left(|b_{k+1}| + ... + |b_d|\right) \\
&= (1 - r)|f(z_0)| + \tfrac{r|f(z_0)|}{|b_k|}|z - z_0|\left(|b_{k+1}| + ... + |b_d|\right) \\
&< (1 - r)|f(z_0)| + \tfrac{r|f(z_0)|}{|b_k|}\tfrac{|b_k|}{|b_{k+1}|+...+|b_d|}\left(|b_{k+1}| + ... + |b_d|\right) \\
&= |f(z_0)| - r|f(z_0)| + r|f(z_0)| \\
&= |f(z_0)|
\end{aligned}$$

to get exactly what we need to complete the proof of the Theorem!

With all big proofs, it is useful to play the devil's advocate and think about settings where the proof couldn't possibly work, because it would prove something false. When you construct your own proofs, this is a good way to detect errors. (If it does prove something false, there must be something wrong with the proof!) But even here, where there are no errors, playing the devil's advocate is useful for exploring the proof.

Devil's Advocate 1: This shouldn't prove that there are **real** roots because, for example, the polynomial $x^2 + 1$ does not have real roots. So what happens to the proof when we replace $\mathbb{C}$ by $\mathbb{R}$? Well, (a) still works, except that in this case a "circle" C of radius R is just the pair of points $R, -R \in \mathbb{R}$. So there must be a global minimum of $|x^2+1|$ inside each interval $[-R, R]$ (and R large). But (b) fails (obviously) since 1 (not 0) is the global minimum for $|x^2 + 1|$. When we investigate the proof, we see that in (b), we assumed we could always solve:

$$z = \sqrt[k]{\frac{-rf(z_0)}{b_k}} + z_0$$

In this case, when $x_0 = 0, f(0) = 1$ and $b_2 = 1$, we are asking to solve:

$$x = \sqrt[2]{-r}$$

which **can't be done** when x is real, though of course it can be done when x is complex! This is why our proof does not (wrongly!) prove that polynomials always have real roots.

Devil's Advocate 2: What about the exponential function from §4?:

$$e^z = e^{x+iy} = e^x e^{iy}$$

We saw that $e^{iy} = \cos(y) + \sin(y)\ i$ so:

$$|e^z| = |e^x||e^{iy}| = e^x(\cos^2(y) + \sin^2(y)) = e^x$$

and this function has **no** "roots." In this case, part (b) of the proof still holds (it only required e^z to have a Taylor series expansion!) and $|e^z|$ has no local (or global) minima inside the disk, but (a) doesn't hold! In fact,

$$|e^z| = e^x$$

gets very **small** on the points of large circles with "large" negative x-coordinates. So on **every** disc D, the global minima of $|e^z|$ occur on the boundary circle C!

2.5.1 Fundamental Theorem of Algebra Exercises

9-1 Prove that **every** complex root α of:

$$f(x) = a_d x^d + ... + a_0$$

satisfies

$$|\alpha| \leq \frac{|a_{d-1}| + ... + |a_0|}{|a_d|} \text{ or } |\alpha| < 1$$

(Hint: You need to modify the proof of (a), replacing $|f(0)|$ with 0)

9-2 Taylor expand the following polynomials about $x = -1$:

(a) $x^2 + 2x + 2$

(b) $x^3 + 3x^2 + 3x + 3$

(c) $x^3 + 4x^2 + 5x + 4$

(d) $x^5 + 1$

Which of these polynomials, thought of as a function $f : \mathbb{R} \to \mathbb{R}$, has a global minimum at $x = -1$? Which has a local minimum at $x = -1$? Which has a critical point at $x = -1$?

9-3 Consider the polynomial:

$$x^2 + 1 \in F_2[x]$$

and attempt a "Taylor expansion" of it at $x = 1$. What happens?

9-4 Use the fundamental theorem to prove:

(a) Every prime polynomial in $\mathbb{Q}[x]$ of degree d has d **different** complex roots. (See also Exercise 7-1(d)). So if the characteristic polynomial of α has degree d, then α has $d - 1$ conjugates.

(b) The **only** prime polynomials in $\mathbb{C}[x]$ are the linear polynomials.

(c) The **only** prime polynomials in $\mathbb{R}[x]$ are the linear polynomials and quadratic polynomials $ax^2 + bx + c$ with $b^2 - 4ac < 0$.

9-5 Prove the triangle inequality:

$$|z + w| \leq |z| + |w|$$

for complex numbers z, w.