COUNTING ROOTS OF POLYNOMIALS

KEITH CONRAD

Every linear polynomial with real coefficients has exactly one real root. From the quadratic formula or the graph of a parabola, every quadratic polynomial with real coefficients has at most two real roots. The number of roots might be less than two: x^2 has only one real root and $x^2 + 1$ has no real roots.

Using algebra, rather than graphs or root formulas, the bound on the number of roots of a polynomial of degree two can be extended to a bound for on the number of roots of a polynomial of any degree with coefficients belonging to any field, not just the real numbers.

Theorem 1. *Let F be a field and $f(T)$ be a non-constant polynomial with coefficients in F, of degree d. Then $f(T)$ has at most d roots in F.*

To prove Theorem 1, we will need a preliminary lemma connecting roots and linear factors.

Lemma 2. *Let $f(T)$ be a non-constant polynomial with coefficients in a field F. For $a \in F$, $f(a) = 0$ if and only if $T - a$ is a factor of $f(T)$.*

Proof. If $T - a$ is a factor of $f(T)$, then $f(T) = (T - a)h(T)$ for some polynomial $h(T)$, and substituting a for T shows $f(a) = 0$.

Conversely, suppose $f(a) = 0$. Write the polynomial as

$$f(T) = c_n T^n + c_{n-1} T^{n-1} + \cdots + c_1 T + c_0, \tag{1}$$

where $c_j \in F$. Then

$$0 = c_n a^n + c_{n-1} a^{n-1} + \cdots + c_1 a + c_0. \tag{2}$$

Subtracting (2) from (1), the terms c_0 cancel and we get

$$f(T) = c_n(T^n - a^n) + c_{n-1}(T^{n-1} - a^{n-1}) + \cdots + c_1(T - a). \tag{3}$$

Since

$$T^j - a^j = (T - a)(T^{j-1} + aT^{j-2} + \cdots + a^i T^{j-1-i} + \cdots + a^{j-2}T + a^{j-1}),$$

each term on the right side of (3) has a factor of $T - a$. Factor this out of each term, and we obtain $f(T) = (T - a)g(T)$, where $g(T)$ is another polynomial with coefficients in F. □

Now we prove Theorem 1.

Proof. We induct on the degree d of $f(T)$. Note $d \geq 1$.

A polynomial of degree 1 has the form $f(T) = aT + b$, where a and b are in F and $a \neq 0$. This has exactly one root in F, namely $-b/a$, and thus *at most* one root in F. That settles the theorem for $d = 1$.

Now assume the theorem is true for all polynomials with coefficients in F of degree d. We verify the theorem for all polynomials with coefficients in F of degree $d + 1$.

A polynomial of degree $d + 1$ is

$$f(T) = c_{d+1} T^{d+1} + c_d T^d + \cdots + c_1 T + c_0, \tag{4}$$

where $c_j \in F$ and $c_{d+1} \neq 0$. If $f(T)$ has no roots in F, then we're done, since $0 \leq d+1$. If $f(T)$ has a root in F, say r, then Lemma 2 tells us $f(T) = (T-r)g(T)$, where $g(T)$ is another polynomial with coefficients in F, of degree d (why degree d?). We can therefore apply the inductive hypothesis to $g(T)$ and conclude that $g(T)$ has at most d roots in F. For every $a \in F$ we have $f(a) = (a-r)g(a)$, and a product of numbers in F is 0 only when one of the factors is 0, so any root of $f(T)$ in F is either r or is a root of $g(T)$. Thus, $f(T)$ has at most $d+1$ roots in F. As $f(T)$ was an arbitrary polynomial of degree $d+1$ with coefficients in F, we are done with the inductive step. □

Remark 3. There were two cases considered in the inductive step: when $f(T)$ has a root in F and when it does not. Certainly one of those cases must occur, but in any particular example we don't know which occurs without actually searching for roots. This is why the theorem is not effective. It gives us an upper bound on the number of roots, but does not give us any tools to decide if there is even one root in F for a particular polynomial.

Remark 4. Using modular arithmetic we can get examples of polynomials with *more* roots than their degree. For example $T^2 - 1$ has four roots in $\mathbf{Z}/(8)$: $1, 3, 5, 7$. This does not contradict Theorem 1 because $\mathbf{Z}/(8)$ is not a field and is not contained in a field since it has zero divisors, such as 2 and 4. The proof of Theorem 1 breaks down in this example because $T^2 - 1 = (T-1)(T+1) = (T-1)g(T)$ and if $(a-1)g(a) = 0$ in $\mathbf{Z}/(8)$ it need not be the case that $a-1$ or $g(a)$ is 0 in $\mathbf{Z}/(8)$: $(3-1)(3+1) = 0$ in $\mathbf{Z}/(8)$ without either factor being 0 in $\mathbf{Z}/(8)$.

As another example, $2T + 2$ has degree 1 and more than 1 root in $\mathbf{Z}/(8)$: 3 and 7. Therefore even the base case of the induction in Theorem 1 doesn't work when we work in $\mathbf{Z}/(8)$.