Factoring a multivariable polynomial

Jordan Hoffart

Theorem 1. *Let p be a real-valued polynomial in 1 variable of degree $k \geq 1$. Then $p(a) = 0$ iff there is a polynomial q of degree $k-1$ such that*

$$p(x) = (x-a)q(x)$$

for all $x \in \mathbb{R}$.

Proof. Fix x and set $h = a - x$. Performing a Taylor expansion of p at x using $x + h$ and using the fact that $p(a) = p(x+h) = 0$ tells us that

$$0 = p(x) + (a-x)p'(x) + \cdots + \frac{(a-x)^k}{k!}p^{(k)}(x).$$

Thus

$$p(x) = (x-a)p'(x) + \cdots + (-1)^{k+1}\frac{(x-a)^k}{k!}p^{(k)}(x).$$

Setting

$$q(x) = p'(x) - \frac{(x-a)}{2}p''(x) + \cdots + (-1)^{k+1}\frac{(x-a)^{k-1}}{k!}p^{(k)}(x)$$

proves one direction. The other direction holds from evaluating at $x = a$. □

Corollary 1. *If p is a degree at most n polynomial that vanishes at $n+1$ points, then $p = 0$.*

Proof. Suppose p vanishes at the points $a_0, \ldots, a_n$. Then since p vanishes at a_n, we have that $p(x) = (x-a_n)q(x)$ where the degree of q is at most $n-1$. Since a_n is distinct from the other a_i but p vanishes at the other a_i, we must have that q is a degree at most $n-1$ polynomial that vanishes at n distinct points. Repeating this argument inductively allows us to conclude that $p(x) = (x-a_n)\cdots(x-a_1)C$ for some constant C. But $p(a_0) = 0$ and a_0 is distinct from the other a_i, so we must have that $C = 0$. Thus $p = 0$ identically. □

Corollary 2. *Let p be a real-valued polynomial in m variables of total degree at most n. If p vanishes at $n+1$ points lying along a straight line, then p vanishes on that line.*

Proof. Parameterize the line with a degree one vector-valued polynomial $r(t)$. Then $p(r(t))$ is a degree at most n polynomial that vanishes at $n+1$ distinct points $t_0, \ldots, t_n$. From the previous corollary, $p(r(t)) = 0$ for all t, which means that $p = 0$ on the line. □

Lemma 1. *Let p be a polynomial in 2 variables of total degree n. Then for $(x, y) \in \mathbb{R}^2$,*

$$p(x+h, y+k) = p(x, y) + \sum_{m=1}^{n} \frac{1}{m!} \sum_{i=0}^{m} \binom{m}{i} \partial_x^{m-i} \partial_y^i p(x, y) h^{m-i} k^i.$$

Proof. Let $r(t) = (x+ht, y+kt)$. Then let $q(t) = p(r(t))$. Then q is a polynomial of degree n in t, so by Taylor's Theorem,

$$q(1) = q(0) + q'(0) + \cdots + \frac{1}{n!} q^{(n)}(0).$$

By the chain rule, we have that

$$\begin{aligned} q'(0) &= \partial_x p(x, y) h + \partial_y p(x, y) k, \\ q''(0) &= \partial_x^2 p(x, y) h^2 + 2\partial_{xy}^2 p(x, y) hk + \partial_y^2 p(x, y) k^2, \\ &\vdots \\ q^{(n)}(0) &= \sum_{i=0}^{n} \binom{n}{i} \partial_x^{n-i} \partial_y^i p(x, y) h^{n-i} k^i. \end{aligned}$$

Putting this altogether gives us the result. □

Theorem 2. *Let p be a real-valued polynomial in 2 variables of total degree $n \geq 1$. Let L be the line consisting of all points (x, y) such that $ax + by + c = 0$. Then p vanishes on L iff there is a polynomial q of total degree $n - 1$ such that*

$$p(x, y) = (ax + by + c) q(x, y)$$

for all $(x, y) \in \mathbb{R}^2$.

Proof. Suppose without loss of generality that $a, b, c, \neq 0$, as these special cases are easier and handled similarly. Fix $(x, y) \in \mathbb{R}^2$ and consider the point $(x, -(ax+c)/b)$ on L with the same x coordinate. Then by applying the previous lemma with $h = 0$ and $k = -(ax + c)/b - y$, we have that

$$0 = p(x, y) + \sum_{m=1}^{n} \frac{1}{m!} \partial_y^m p(x, y) (-1)^m ((ax + c)/b + y)^m.$$

Therefore, after rearranging and factoring a term,

$$p(x, y) = (ax + by + c) \frac{1}{b} \sum_{m=1}^{n} \frac{(-1)^{m+1}}{m!} \partial_y^m p(x, y) (y + (ax + c)/b)^{m-1}.$$

Setting

$$q(x, y) = \frac{1}{b} \sum_{m=1}^{n} \frac{(-1)^{m+1}}{m!} \partial_y^m p(x, y) (y + (ax + c)/b)^{m-1}$$

proves one direction. The other direction holds by evaluating at a point on L. □

Corollary 3. *If a degree $n \geq 1$ polynomial p in 2 variables vanishes at $n+1$ points that lie on a straight line, and if the line is characterized as the set of solutions to $L(x,y) = 0$ for a degree one polynomial L, then $p(x,y) = L(x,y)q(x,y)$ for some degree $n-1$ polynomial q.*

Corollary 4. *If a degree $n \geq 1$ polynomial in 2 variables takes the same value C at $n+1$ points that lie on a straight line, and if the line is characharacterized as the set of solutions to $L(x,y) = 0$ for a degree one polynomial L, then $p(x,y) = L(x,y)q(x,y) + C$ for some degree $n-1$ polynomial q.*

Proof. Apply the previous corollary to the polynomial $r(x,y) = p(x,y) - C$. $\square$