Permutations and Polynomials

Sarah Kitchen

February 7, 2006

Suppose you are given the equations $x + y + z = a$ and $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{1}{a}$, and are asked to prove that one of x,y, and z is equal to a. We are used to solving problems of this type by finding out where the graphs of those equations intersect– i.e. by solving for one variable in terms of the others and checking a bunch of cases.

To illustrate, try solving the above problem algebraically for $a = 2$. That is, if $x + y + z = 2$ and $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{1}{2}$, show x or y or z must equal 2.

I claim that one of x, y, and z must be equal to a because a is a root of the polynomial $p(t) = t^3 - at^2 + bt - ab$ for any b. This solution is much faster, but it is not at all obvious why this observation leads to our desired conclusion. The idea is to find b such that x, y, and z are all the roots of $p(t)$. Then, since a is also a root, a must coincide with one of x, y, and z. But how do we find such a b? To investigate, we will explore the general relationship between the roots of a polynomial and its coefficients.

Definition: A polynomial in n variables is *homogeneous of degree k* if all the monomials have degrees which sum to k.

Examples:

1. $p(x) = x$ is a homogeneous polynomial of degree 1 in one variable.
2. $q(x, y, z) = x^4 + y^2z^2$ is a homogeneous polynomial of degree 4 in three variables.
3. $r(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$ is a homogeneous polynomial of degree 2 in four variables.

We notice something special about the polynomial $r(x_1, x_2, x_3, x_4)$. If we swap x and z in $q(x, y, z)$, we find $q(z, y, x) = z^4 + y^2x^2$ is not the same polynomial as $q(x, y, z)$, but no matter how we reorder the x_i, r remains the same.

Definition: A *permutation* is a function σ which reorders a list of objects.

For example, let σ be the permutation on the numbers $\{1,\ 2,\ 3,\ 4\}$ such that $\sigma(1) = 1$, $\sigma(2) = 4$, $\sigma(3) = 2$, $\sigma(4) = 3$. We see that σ reorders the list $\{1,\ 2,\ 3,\ 4\}$ as $\{1,\ 4,\ 2,\ 3\}$. With this new notation, our observation about r above can be re-stated as follows: For any permutation σ of $\{1,\ 2,\ 3,\ 4\}$, we have

$$r(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)}) = r(x_1, x_2, x_3, x_4).$$

We give the following name to polynomials with this property:

Definition: A polynomial p in n variables, $x_1, x_2, \ldots, x_n$ is *symmetric* if for any permutation σ on $\{1,\ 2, \ldots,\ n\}$,

$$p(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = p(x_1, x_2, \ldots, x_n).$$

Exercise: Is $p(x, y, z) = x + y + z$ symmetric? Is $p(x, y, z) = x + y$?

There is a special collection of symmetric polynomials, called *elementary symmetric polynomials*. The kth elementary symmetric polynomial in n variables, denoted $s_k(x_1, \ldots, x_n)$, is the sum of all possible degree k monomials in n variables with each x_i appearing no more than once in each monomial. Formally, for $k \leq n$, we will write

$$s_k(x_1, \ldots, x_n) = \sum_{1 \leq i_1 < \ldots < i_k \leq n} x_{i_1} x_{i_2} \ldots x_{i_k}$$

Example: $p(x, y) = xy^2 + yx^2$ is symmetric and homogeneous, but *not* an elementary symmetric polynomial. The polynomial $r(x_1, x_2, x_3, x_4)$ above *is* an elementary symmetric polynomial.

Exercises:

1. How many monomials are there in the elementary symmetric polynomial of degree k in n variables?

2. List all the monomials of degree 3 in 4 variables.

3. Write down the elementary symmetric polynomials of all degrees in 3 variables.

You may have learned in algebra while learning how to factor polynomials that any integer root of a polynomial with integer coefficients will divide the degree zero term. Here is an explaination of why this should be so: Suppose a and b are roots of $x^2 - cx + d$. Since we know the roots, we know how factor this polynomial as $(x-a)(x-b)$. When we multiply out the factors, we see

$$x^2 - (a+b)x + ab = x^2 - cx + d;$$

consequently, $a + b = c$ and $ab = d$, so a and b must divide d.

Observe further that $a + b = s_1(a, b)$ and $ab = s_2(a, b)$, so we can rewrite the polynomial

$$x^2 - cx + d = x^2 - (a+b)x + ab = x^2 - s_1(a,b)x + s_2(a,b).$$

It happens to be true in general, that if $a_1, a_2, \ldots, a_n$ are the roots of a degree n polynomial $p(x)$, of the form $p(x) = x^n + \alpha_{n-1}x^{n-1} + \ldots + \alpha_0$, then

$$p(x) = \prod_{i=1}^{n}(x - a_i) = x^n + \sum_{i=1}^{n}(-1)^i s_i(a_1, \ldots, a_n)x^{n-i}. \tag{1}$$

This implies that the coefficients $\alpha_i = (-1)^i s_i(a_1, \ldots, a_n)$. In other words, the coefficients of a polynomial can be written explicitly in terms of the roots of that polynomial using the elementary symmetric polynomials.

Example:

$$(x-a)(x-b)(x-c) = x^3 - (a+b+c)x^2 + (ab+bc+ac)x - abc$$

Exercises: Compute the following polynomials in two ways– multiplying everything out manually first, then computing the coefficients via the elementary symmetric polynomials to verify they yield the same answer.

1. $(x-1)(x-2)(x-3)$

2. $(x-1)(x+2)(x-3)$

3. $(x-2)^3(x-3)^2$

4. $(x-\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3})(x+\sqrt{2}-\sqrt{3})(x+\sqrt{2}+\sqrt{3})$

With a little practice, you will find you can expand factored polynomials *very quickly* with this trick. Amaze your friends and family!

We are ready to return to our original problem. Let $b = xy + xz + yz$ and $p(t) = (t - x)(t - y)(t - z)$. Then,

$$\frac{1}{a} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{yz + xz + xy}{xyz} = \frac{b}{xyz}$$

which implies $xyz = ab$. Therefore,

$$p(t) = t^3 - (x + y + z)t^2 + (xy + xz + yz)t - (xyz) = t^3 - at^2 + bt - ab.$$

On the other hand, recall $p(a) = a^3 - a(a^2) + b(a) - ab = 0$, so a is a root of p. Therefore, a must equal x, y, or z.

Exercises: Solve the following problems using elementary symmetric polynomials.

1. Find a, b, c such that the roots of $f(x) = x^3 + ax^2 + bx + c$ are a, b, c.

2. Let a_1, a_2, a_3 be roots of $6x^3 - 2x^2 + 3x + 5$. Find a polynomial with roots $\frac{1}{a_1}, \frac{1}{a_2}, \frac{1}{a_3}$.

3. Let a_1, a_2, a_3 be roots of $2x^3-7x+8$. Find a polynomial with roots $\frac{1}{a_1a_2}, \frac{1}{a_2a_3}, \frac{1}{a_1a_3}$.

4. Let a_1, a_2, a_3 be the three roots of $x^3 + 3x + 1$.

   (a) Find a polynomial with roots a_1^2, a_2^2, a_3^2.

   (b) Find a polynomial with roots $a_1 + a_2, a_1 + a_3, a_2 + a_3$.

5. The Wicked Witch said that the following polynomial has 2005 integer roots: $x^{2005} + 2x^{2004} + 3x^{2003} + \ldots$. Prove she is a liar. Hint: You will need the following relation:

$$x_1^2 + x_2^2 + \ldots + x_n^2 = s_1(x_1, \ldots, x_n)^2 - 2s_2(x_1, \ldots, x_n)$$

For the interested reader, here is the proof of equation 1. The proof is by induction on the degree of the polynomial. If our polynomial is of degree $n = 1$ with root a, the left hand side is $x - a$, and the right hand side is $x - s_1(a) = x - a$, so the equation holds for $n = 1$. Suppose the equation holds for all polynomials of degree n. Let $p(x)$ be of degree $n + 1$ with roots $a_1, \ldots, a_{n+1}$. Then, we can write

$$p(x) = (x - a_{n+1}) \prod_{i=1}^{n} (x - a_i) = (x - a_{n+1})(x^n + \sum_{i=1}^{n} (-1)^i s_i x^{n-i}),$$

where we let s_i denote $s_i(a_1, \ldots, a_n)$ for brevity. By multiplying out the right hand side:

$$p(x) = x^{n+1} - (s_1 + a_{n+1})x^n + \sum_{i=1}^{n-1} (-1)^{i+1}(s_{i+1} + a_{n+1}s_i)x^{n-i} + (-1)^{n+1}a_{n+1}s_n$$

Since

$$s_1 + a_{n+1} = (a_1 + \ldots + a_n) + a_{n+1} = s_1(a_1, \ldots, a_{n+1})$$

and

$$s_n a_{n+1} = (a_1 a_2 \ldots a_n)a_{n+1} = s_{n+1}(a_1, \ldots, a_n, a_{n+1}),$$

if we can show $s_{i+1} + s_i a_{n+1} = s_{i+1}(a_1, \ldots, a_{n+1})$ for all the other i, we conclude the equation holds for $n + 1$, hence for all n. By definition,

$$s_{i+1}(a_1, \ldots, a_{n+1}) = \sum_{1 \leq j_1 < \ldots < j_{i+1} \leq n+1} a_{j_1} a_{j_2} \ldots a_{j_{i+1}}$$

By separating the sum with respect to monomials divisible by a_{n+1}, we see the above is equal to

$$\sum_{1 \leq j_1 < \ldots < j_{i+1} \leq n} a_{j_1} a_{j_2} \ldots a_{j_{i+1}} \quad + a_{n+1} \sum_{1 \leq j_1 < \ldots < j_i \leq n} a_{j_1} a_{j_2} \ldots a_{j_i} = s_{i+1} + a_{n+1}s_i$$

so it is clear the relationship we wanted holds.