**Levels recommended:** 5-7

Before we state the theorem, we need some definitions.

Suppose we have n variables $x_1, x_2, x_3, \dots, x_n$. Then $s_k$ is defined as the sum of all products of k different variables. For example, $s_3 = x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n$.

These are called **elementary symmetric polynomials**. Note that $s_k$ is exactly the coefficient of $x^{n-k}$ in the polynomial $(x + x_1)(x + x_2)(x + x_3) \dots (x + x_n)$. So if $x_1, x_2, x_3, \dots, x_n$ were the actual roots, we would have the known result that the s's are the coefficients up to possibly a change in the sign. We will use this result in the application after the proof.

A **symmetric polynomial** is a function of more than one variables such that the function is obtained by only adding and multiplying the variables, and it has the property that if you input them in a different order you get the same function.

For example, $f(x, y, z) = x^2yz + xy^2z + xyz^2$ is a symmetric polynomial. This is because it is sums of products of x, y and z and $f(x, y, z) = f(x, z, y) = f(y, x, z) = f(y, z, x) = f(z, x, y) = f(z, y, x)$. However, something like $x^2 + y^2 - z^2$ is not symmetric as if you swap y and z you do not have the same function.

Note that our example $x^2yz + xy^2z + xyz^2 = s_1s_3$. This is a special case of the theorem.

**Theorem** (the fundamental theorem of symmetric polynomials: All symmetric polynomials can be written as sums of products of elementary symmetric polynomials.

**Proof:**

**Lemma:** Suppose we have finite ordered lists of non-negative integers. Define an ordering on these lists where we say one list is greater than another if its first element is greater. If the first element is the same, say one list is greater if its second element is greater, and so on. Then the lemma claims that if I start with such a list, there is no infinitely decreasing chain of such lists.

**Proof of lemma:** Lets go by induction. We know for sure that for lists of 1 number this is true. For any number I start with I clearly cannot make an infinitely decreasing chain of non-negative integers starting from that number. Now suppose it is true for k numbers. Then for a (k+1)-list, what happens is that I must decrease the first number after finitely many steps, because if I try to decrease the list, then by the induction hypothesis, after finitely many steps I will not be able to decrease the elements from positions 2 to k+1 anymore. At that point I will have to decrease the first element. But then this is a finite thing that happens finitely many times. So done.

Now let's prove the main theorem.

Lets take each term in a symmetric polynomial like $Cx_1^{d_1}x_2^{d_2} \dots x_n^{d_n}$ and define the multidegree of that term as the list $(d_1, d_2, \dots, d_n)$, where some terms may be 0. Sort the terms from largest to smallest multidegree where the ordering of the multidegree is as in the statement of the lemma.

Note that the list of the multidegree of the term with largest multidegree will be in decreasing order. This is because if it was not, we could sort it into decreasing order and by symmetry of the polynomial that term must be one of the terms, and by how the ordering works it would have a larger multidegree so any unsorted list could not be the largest multidegree.

Note that the term with the largest multidegree in the product of symmetric polynomials is the product of the terms with the largest multidegree in the symmetric polynomials we are multiplying. This is because by how the ordering on the multidegree works, and the fact multiplying by any term just adds constants to the multidegree, multiplying by any term will not affect the ordering. If we let Y be the multidegree of the product of the terms in the polynomials we are multiplying that have largest multidegree, then all other terms in the polynomials will have lower multidegree so their product will have lower multidegree than Y – never higher – so Y is the largest.

Now consider $s_n^{d_n} s_{n-1}^{d_{n-1}-d_n} s_{n-2}^{d_{n-2}-d_2} \dots s_2^{d_2-d_3} s_1^{d_3-d_2}$. Then the highest multidegree term in each of the terms we are multiplying will be $(d_n, d_n, \dots, d_n), (d_{n-1}-d_n, d_{n-1}-d_n, \dots, d_{n-1}-d_n, 0), \dots,$

$(d_2-d_3, d_2-d_3, 0, \dots, 0), (d_1-d_2, 0, \dots, 0)$, so the term with highest multidegree in the product will have multidegree $(d_1, d_2, \dots, d_n)$.

Therefore let $P(x_1, x_2, \dots, x_n)$ be a symmetric polynomial whose term with largest multidegree is $Cx_1^{d_1} x_2^{d_2} \dots x_n^{d_n}$. Then $P(x_1, x_2, \dots, x_n) - Cs_n^{d_n} s_{n-1}^{d_{n-1}-d_n} s_{n-2}^{d_{n-2}-d_2} \dots s_2^{d_2-d_3} s_1^{d_1-d_2}$ is a symmetric polynomial whose largest multidegree is at most $(d_1, d_2, \dots, d_n)$. But it is actually not that as by construction the terms with that multidegree cancelled. So the largest multidegree is something lower. Lets call this new polynomial $Q(x_1, x_2, \dots, x_n)$ and do the same procedure. But each time we do this, the largest multidegree decreases, so after finitely many steps it will be down to 0 by the lemma. So eventually we will have $P(x_1, x_2, \dots, x_n) - Cs_n^{d_n} s_{n-1}^{d_{n-1}-d_n} s_{n-2}^{d_{n-2}-d_2} \dots s_2^{d_2-d_3} s_1^{d_1-d_2} -$ $(More\ sums\ and\ products\ of\ symmetric\ polynomials) = Constant$. So move everything but P to 1 side then we are done.

**Example:**

Suppose that the following is true:

$$x + y + z = 1$$

$$x^2 + y^2 + z^2 = 2$$

$$x^3 + y^3 + z^3 = 3$$

And we want $x^4 + y^4 + z^4$.

Then lets write $x^2 + y^2 + z^2$ in terms of the s's. Write it as $x^2y^0z^0 + x^0y^2z^0 + x^0y^0z^2$. The largest multidegree is (2,0,0) so by the proof we want to try subtracting $s_1^2$.

$$x^2 + y^2 + z^2 - s_1^2 = -2xy - 2yz - 2xz$$

Now we have reduced the largest multidegree to (1,1,0). In this case we want to add $2s_2$ to both sides, then we will get $x^2 + y^2 + z^2 - s_1^2 + 2s_2 = 0$ so

$$x^2 + y^2 + z^2 = s_1 - 2s_2$$

But $s_1 = 1$ from the first equation and $s_1 - 2s_2 = 2$ from the second one. Therefore $s_2 = -\frac{1}{2}$.

We can do the same procedure and it turns out that

$$x^3 + y^3 + z^3 - s_1^3 = -3x^2y - 3x^2z - 3y^2x - 3y^2z - 3z^2x - 3z^2y - 6xyz$$

$$x^3 + y^3 + z^3 - s_1^3 + 3s_1s_2 = 3xyz$$

$$x^3 + y^3 + z^3 = s_1^3 - 3s_1s_2 + 3s_3$$

So $s_3 = \frac{1}{6}$.

We could try to express $x^4 + y^4 + z^4$ in terms of elementary symmetric polynomials the same way and then solve for this. If we do this we get $\frac{25}{6}$.

**Application (In mathematics, not the real world, don't worry):**

Suppose we want to find a polynomial with integer coefficients such that $2^{\frac{1}{2}} + 3^{\frac{1}{3}}$ is a root, or more generally the sum of the roots of any two other polynomials is a root. The above are roots of $x^2 - 2$ and $x^3 - 3$ respectively. Let the roots of $x^2 - 2$ be $x_1, x_2$ and the roots of $x^3 - 3$ be $y_1, y_2, y_3$, then there is a polynomial whose roots are all the possible sums of roots of the two polynomials, ie a polynomial whose roots are $x_1 + y_1, x_2 + y_2, x_1 + y_2, x_2 + y_1, x_1 + y_3, x_2 + y_3$. Lets call these $z_1, z_2, \dots, z_6$. Then notice that $(x - z_1)(x - z_2) \dots (x - z_6)$'s coefficients are exactly the symmetric polynomials in the z variables. But then we can substitute back in x and y. The coefficients will then be symmetric polynomials in the x and y variables. These can be expressed in terms of the elementary ones, which are integers, because they are (possibly with a sign change) the coefficients of the starting polynomials, ie $x^2 - 2$ and $x^3 - 3$. So $(x - z_1)(x - z_2) \dots (x - z_6)$ has integer coefficients and has $2^{\frac{1}{2}} + 3^{\frac{1}{3}}$ as a root. $x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1$ is the expanded polynomial, by the way, which indeed has $2^{\frac{1}{2}} + 3^{\frac{1}{3}}$ as one of its roots. We could find this but it would take a lot of annoying work. The same applies to products of two roots.

So, if you know what a ring is, now you know that algebraic numbers are closed under addition and (by a similar argument) multiplication and thus they are a ring.