SYMMETRIC POLYNOMIALS

KEITH CONRAD

Let F be a field. A polynomial $f(T_1, \ldots, T_n) \in F[T_1, \ldots, T_n]$ is called *symmetric* if it is unchanged by any permutation of its variables:

$$f(T_1, \ldots, T_n) = f(T_{\sigma(1)}, \ldots, T_{\sigma(n)})$$

for all $\sigma \in S_n$.

Example 1. The sum $T_1 + \cdots + T_n$ and product $T_1 \cdots T_n$ are symmetric, as are the power sums $T_1^r + \cdots + T_n^r$ for any $r \geq 1$.

As a measure of how symmetric a polynomial is, we introduce an action of S_n on $F[T_1, \ldots, T_n]$:

$$(\sigma f)(T_1, \ldots, T_n) = f(T_{\sigma^{-1}(1)}, \ldots, T_{\sigma^{-1}(n)}).$$

We need σ^{-1} rather than σ on the right side so this is a group action (*i.e.*, so that $\sigma(\tau f)$ equals $(\sigma\tau)(f)$ rather than $(\tau\sigma)(f)$). The action of S_n on $F[T_1, \ldots, T_n]$ is not only permutations of $F(T_1, \ldots, T_n)$ but ring automorphisms fixing F:

$$\sigma(f + g) = \sigma f + \sigma g, \quad \sigma(fg) = (\sigma f)(\sigma g), \quad \sigma(c) = c$$

for polynomials f and g and constants $c \in F$.

Example 2. Let $f(T_1, T_2, T_3) = T_1^5 + T_2 T_3$. If $\sigma = (123)$ then $\sigma f = f(T_3, T_1, T_2) = T_3^5 + T_1 T_2$. If $\sigma = (23)$ then $\sigma f = f$. That f is fixed by a nontrivial subgroup of S_3 makes it "partially symmetric."

A polynomial f in n variables is symmetric when $\sigma f = f$ for all $\sigma \in S_n$.

An important collection of symmetric polynomials occurs as the coefficients in the polynomial

$$(X - T_1)(X - T_2) \cdots (X - T_n) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \cdots + (-1)^n s_n. \tag{1}$$

Here s_1 is the sum of the T_i's, s_n is their product, and more generally

$$s_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} T_{i_1} \cdots T_{i_k}$$

is the sum of the products of the T_i's taken k terms at a time. The s_k's are all symmetric in $T_1, \ldots, T_n$ and are called the *elementary* symmetric polynomials – or elementary symmetric functions – in the T_i's

Example 3. Let $\alpha = \frac{3+\sqrt{5}}{2}$ and $\beta = \frac{3-\sqrt{5}}{2}$. Although α and β are not rational, their elementary symmetric polynomials are: $s_1 = \alpha + \beta = 3$ and $s_2 = \alpha\beta = 1$.

Example 4. Let α, β, and γ be the three roots of $X^3 - X - 1$, so

$$X^3 - X - 1 = (X - \alpha)(X - \beta)(X - \gamma).$$

Multiplying out the right side and equating coefficients on both sides, the elementary symmetric polynomials in α, β, and γ are $s_1 = \alpha + \beta + \gamma = 0$, $s_2 = \alpha\beta + \alpha\gamma + \beta\gamma = -1$, and $s_3 = \alpha\beta\gamma = 1$.

Theorem 5. *The set of symmetric polynomials in $F[T_1, \ldots, T_n]$ is $F[s_1, \ldots, s_n]$. That is, every symmetric polynomial in n variables is a polynomial in the elementary symmetric functions of those n variables.*

Example 6. In two variables, the polynomial $X^3 + Y^3$ is symmetric in X and Y. As a polynomial in $X + Y$ and XY,

$$X^3 + Y^3 = (X + Y)^3 - 3XY(X + Y) = s_1^3 - 3s_1s_2.$$

Our proof of Theorem 5 will proceed by induction on the multi-degree of a polynomial in several variables, which is defined in terms of a certain ordering on multivariable polynomials, as follows.

Definition 7. For two vectors $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{b} = (b_1, \ldots, b_n)$ in $\mathbf{N}^n$, set $\mathbf{a} < \mathbf{b}$ if, for the first i such that $a_i \neq b_i$, we have $a_i < b_i$.

Example 8. In $\mathbf{N}^4$, $(3, 0, 2, 4) < (5, 1, 1, 3)$ and $(3, 0, 2, 4) < (3, 0, 3, 1)$.

For any two n-tuples $\mathbf{a}$ and $\mathbf{b}$ in $\mathbf{N}^n$, either $\mathbf{a} = \mathbf{b}$, $\mathbf{a} < \mathbf{b}$, or $\mathbf{b} < \mathbf{a}$, so $\mathbf{N}^n$ is totally ordered under $<$. (For example, $(0, 0, \ldots, 0) < \mathbf{a}$ for all $\mathbf{a} \neq (0, 0, \ldots, 0)$.) It is simple to check that for $\mathbf{a}$, $\mathbf{i}$, and $\mathbf{j}$ in $\mathbf{N}^n$,

$$\mathbf{i} < \mathbf{a} \Longrightarrow \mathbf{i} + \mathbf{j} < \mathbf{a} + \mathbf{j}. \tag{2}$$

A polynomial $f \in F[T_1, \ldots, T_n]$ can be written in the form

$$f(T_1, \ldots, T_n) = \sum_{i_1, \ldots, i_n} c_{i_1, \ldots, i_n} T_1^{i_1} \cdots T_n^{i_n}.$$

We will abbreviate this in multi-index form to $f = \sum_{\mathbf{i}} c_{\mathbf{i}} T^{\mathbf{i}}$, where $T^{\mathbf{i}} := T_1^{i_1} \cdots T_n^{i_n}$ for $\mathbf{i} = (i_1, \ldots, i_n)$. Note $T^{\mathbf{i}} T^{\mathbf{j}} = T^{\mathbf{i}+\mathbf{j}}$.

Definition 9. For a nonzero polynomial $f \in F[T_1, \ldots, T_n]$, write $f = \sum_{\mathbf{i}} c_{\mathbf{i}} T^{\mathbf{i}}$. Set the *multi-degree* of f to be

$$\operatorname{mdeg} f = \max\{\mathbf{i} : c_{\mathbf{i}} \neq \mathbf{0}\} \in \mathbf{N}^n.$$

The multi-degree of the zero polynomial is not defined. If $\operatorname{mdeg} f = \mathbf{a}$, we call $c_{\mathbf{a}} T^{\mathbf{a}}$ the *leading term* of f and $c_{\mathbf{a}}$ the *leading coefficient* of f, written $c_{\mathbf{a}} = \operatorname{lead} f$.

Example 10. $\operatorname{mdeg}(T_1 T_2^5 + 3T_2) = (1, 5)$.

Example 11. $\operatorname{mdeg}(T_1) = (1, 0, \ldots, 0)$ and $\operatorname{mdeg}(T_n) = (0, 0, \ldots, 1)$.

Example 12. The multi-degrees of the elementary symmetric polynomials are $\operatorname{mdeg}(s_1) = (1, 0, 0, \ldots, 0)$, $\operatorname{mdeg}(s_2) = (1, 1, 0, \ldots, 0)$, and $\operatorname{mdeg}(s_n) = (1, 1, 1, \ldots, 1)$. The leading term of s_k is $T_1 \cdots T_k$, so the leading coefficient of s_k is 1.

Example 13. Polynomials with multidegree $(0, 0, \ldots, 0)$ are the nonzero constants.

Remark 14. There is a simpler notion of "degree" of a multivariable polynomial: the largest sum of exponents of a nonzero monomial in the polynomial, *e.g.*, $T_1 T_2^3 + T_1^2$ has degree 4. This degree has values in $\mathbf{N}$ rather than $\mathbf{N}^n$. We won't be using it; the multi-degree is more convenient for our purposes.

Our definition of multi-degree is specific to calling T_1 the "first" variable and T_n the "last" variable. Despite its *ad hoc* nature (there is nothing intrinsic about making T_1 the "first" variable), the multi-degree is useful since it permits us to prove theorems about all multivariable polynomials by induction on the multi-degree.

The following lemma shows that a number of standard properties of the degree of polynomials in one variable carry over to multi-degrees of multivariable polynomials.

Lemma 15. *For nonzero f and g in $F[T_1, \ldots, T_n]$, $\operatorname{mdeg}(fg) = \operatorname{mdeg}(f) + \operatorname{mdeg}(g)$ in $\mathbf{N}^n$ and $\operatorname{lead}(fg) = (\operatorname{lead} f)(\operatorname{lead} g)$.*

For f and g in $F[T_1, \ldots, T_n]$, $\operatorname{mdeg}(f + g) \leq \max(\operatorname{mdeg} f, \operatorname{mdeg} g)$ and if $\operatorname{mdeg} f < \operatorname{mdeg} g$ then $\operatorname{mdeg}(f + g) = \operatorname{mdeg} g$.

Proof. We will prove the first result and leave the second to the reader.

Let $\operatorname{mdeg} f = \mathbf{a}$ and $\operatorname{mdeg} g = \mathbf{b}$, say $f = c_{\mathbf{a}} T^{\mathbf{a}} + \sum_{\mathbf{i} < \mathbf{a}} c_{\mathbf{i}} T^{\mathbf{i}}$ with $c_{\mathbf{a}} \neq 0$ and $g = d_{\mathbf{b}} T^{\mathbf{b}} + \sum_{\mathbf{j} < \mathbf{b}} d_{\mathbf{j}} T^{\mathbf{j}}$ with $d_{\mathbf{b}} \neq 0$. This amounts to pulling out the top multi-degree terms of f and g. Then fg has a nonzero term $c_{\mathbf{a}} d_{\mathbf{b}} T^{\mathbf{a}+\mathbf{b}}$ and every other term has multi-degree $\mathbf{a}+\mathbf{j}$, $\mathbf{b}+\mathbf{i}$, or $\mathbf{i}+\mathbf{j}$ where $\mathbf{i} < \mathbf{a}$ and $\mathbf{j} < \mathbf{b}$. By (2), all these other multi-degrees are less than $\mathbf{a}+\mathbf{b}$, so $\operatorname{mdeg}(fg) = \mathbf{a}+\mathbf{b} = \operatorname{mdeg} f + \operatorname{mdeg} g$ and $\operatorname{lead}(fg) = c_{\mathbf{a}} d_{\mathbf{b}} = (\operatorname{lead} f)(\operatorname{lead} g)$. ☐

Now we are ready to prove Theorem 5.

Proof. We want to show every symmetric polynomial in $F[T_1, \ldots, T_n]$ is a polynomial in $F[s_1, \ldots, s_n]$. We can ignore the zero polynomial. Our argument is by induction on the multidegree. Multidegrees are totally ordered, so it makes sense to give a proof using induction on them. A polynomial with multidegree $(0, 0, \ldots, 0)$ is constant, and constants are in $F[s_1, \ldots, s_n]$.

Now pick an $\mathbf{e} \neq (0, 0, \ldots, 0)$ in $\mathbf{N}^n$ and suppose the theorem is proved for all symmetric polynomials with multi-degree less than $\mathbf{e}$. Write $\mathbf{e} = (e_1, \ldots, e_n)$. Pick any symmetric polynomial f with multidegree $\mathbf{e}$. (If there aren't any symmetric polynomials with multi-degree $\mathbf{e}$, then there is nothing to do and move on the next n-tuple in the total ordering on $\mathbf{N}^n$.)

Pull out the leading term of f:

$$f = c_{\mathbf{e}} T_1^{e_1} \cdots T_n^{e_n} + \sum_{\mathbf{i} < \mathbf{e}} c_{\mathbf{i}} T^{\mathbf{i}}, \tag{3}$$

where $c_{\mathbf{e}} \neq 0$. We will find a polynomial in $s_1, \ldots, s_n$ with the same leading term as f. Its difference with f will then be symmetric with smaller multi-degree than $\mathbf{e}$, so by induction we'll be done.

By Example 12 and Lemma 15, for any nonnegative integers $a_1, \ldots, a_n$,

$$\operatorname{mdeg}(s_1^{a_1} s_2^{a_2} \cdots s_n^{a_n}) = (a_1 + a_2 + \cdots + a_n, a_2 + \cdots + a_n, \ldots, a_n).$$

The ith coordinate here is $a_i + a_{i+1} + \cdots + a_n$. To make this multidegree equal to $\mathbf{e}$, we must set

$$a_1 = e_1 - e_2, \quad a_2 = e_2 - e_3, \quad \ldots, \quad a_{n-1} = e_{n-1} - e_n, \quad a_n = e_n. \tag{4}$$

But does this make sense? That is, do we know that $e_1 - e_2, e_2 - e_3, \ldots, e_{n-1} - e_n, e_n$ are all nonnegative? If that isn't true then we have a problem. So we need to show the coordinates in $\mathbf{e}$ satisfy

$$e_1 \geq e_2 \geq \cdots \geq e_n \geq 0. \tag{5}$$

In other words, an n-tuple which is a multi-degree of a symmetric polynomial has to satisfy (5).

To appreciate this issue, consider $f = T_1T_2^5 + 3T_2$. The multi-degree of f is $(1,5)$, so the exponents *don't* satisfy (5). But this f is *not* symmetric, and that is the key point. If we took $f = T_1T_2^5 + T_1^5T_2$ then f is symmetric and $\operatorname{mdeg} f = (5,1)$ does satisfy (5). The verification of (5) will depend crucially on f being a *symmetric* polynomial.

Since $(e_1, \ldots, e_n)$ is the multi-degree of a nonzero monomial in f, and f is symmetric, every vector with the e_i's permuted is *also* a multi-degree of a nonzero monomial in f. (Here is where the symmetry of f in the T_i's is used: under any permutation of the T_i's, f stays unchanged.) Since $(e_1, \ldots, e_n)$ is the largest multi-degree of the monomials in f, $(e_1, \ldots, e_n)$ must be larger in $\mathbf{N}^n$ than all of its nontrivial permutations, which means

$$e_1 \geq e_2 \geq \cdots \geq e_n \geq 0.$$

That shows the definition of $a_1, \ldots, a_n$ in (4) has nonnegative values, so $s_1^{a_1} \cdots s_n^{a_n}$ is a polynomial. Its multidegree is the same as that of f by (4). Moreover, by Lemma 15,

$$\operatorname{lead}(s_1^{a_1} \cdots s_n^{a_n}) = (\operatorname{lead} s_1)^{a_1} \cdots (\operatorname{lead} s_k)^{a_k} = 1.$$

Therefore f and $c_{\mathbf{e}} s_1^{a_1} \cdots s_n^{a_n}$, where $c_{\mathbf{e}} = \operatorname{lead} f$, have the same top multi-degree term. If $f = c_{\mathbf{e}} s_1^{a_1} \cdots s_n^{a_n}$ then we're done. If $f \neq c_{\mathbf{e}} s_1^{a_1} \cdots s_n^{a_n}$ then the difference $f - c_{\mathbf{e}} s_1^{a_1} \cdots s_n^{a_n}$ is nonzero with

$$\operatorname{mdeg}(f - c_{\mathbf{e}} s_1^{a_1} \cdots s_n^{a_n}) < \mathbf{e},$$

and $f - c_{\mathbf{e}} s_1^{a_1} \cdots s_n^{a_n}$ is symmetric since both terms in the difference are symmetric. By induction on the multi-degree, $f - c_{\mathbf{e}} s_1^{a_1} \cdots s_n^{a_n} \in F[s_1, \ldots, s_n]$, so $f \in F[s_1, \ldots, s_n]$. $\square$

Example 16. In three variables, let $f(X,Y,Z) = X^4 + Y^4 + Z^4$. We want to write this as a polynomial in the elementary symmetric polynomials in X, Y, and Z. Treating X, Y, Z as T_1, T_2, T_3, the multidegree of $s_1^a s_2^b s_3^c$ is $(a+b+c, b+c, c)$.

The leading term of f is X^4, with multidegree $(4,0,0)$. This is the multidegree of $s_1^4 = (X+Y+Z)^4$, which has leading term X^4. So we subtract:

$$\begin{aligned} f - s_1^4 &= -4x^3y - 4x^3z + -6x^2y^2 - 12x^2yz - 6x^2z^2 - 4xy^3 - 12xy^2z - 12xyz^2 \\ &\quad -4xz^3 - 4y^3z - 6y^2z^2 - 4yz^3. \end{aligned}$$

This has leading term $-4x^3y$, with multidegree $(3,1,0)$. This is $(a+b+c, b+c, c)$ when $c = 0$, $b = 1$, $a = 2$. So we add $4s_1^a s_2^b s_3^c = 4s_1^2 s_2$ to $f - s_1^4$ to cancel the leading term:

$$f - s_1^4 + 4s_1^2 s_2 = 2x^2y^2 + 8x^2yz + 2x^2z^2 + 8xy^2z + 8xyz^2 + 2y^2z^2,$$

whose leading term is $2x^2y^2$ with multidegree $(2,2,0)$. This is $(a+b+c, b+c, c)$ when $c = 0$, $b = 2$, $a = 0$. So we subtract $2s_2^2$:

$$f - s_1^4 + 4s_1^2 s_2 - 2s_2^2 = 4x^2yz + 4xy^2z + 4xyz^2.$$

The leading term is $4x^2yz$, which has multidegree $(2,1,1)$. This is $(a+b+c, b+c, c)$ for $c = 1$, $b = 0$, and $a = 1$, so we subtract $4s_1s_3$:

$$f - s_1^4 + 4s_1^2 s_2 - 2s_2^2 - 4s_1s_3 = 0.$$

Thus

$$X^4 + Y^4 + Z^4 = s_1^4 - 4s_1^2 s_2 + 2s_2^2 + 4s_1s_3.$$

Corollary 17. *Let L/K be a field extension and $f(X) \in K[X]$ factor as*

$$(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)$$

in $L[X]$. Then for all positive integers r,

$$(X-\alpha_1^r)(X-\alpha_2^r)\cdots(X-\alpha_n^r) \in K[X].$$

Proof. The coefficients of $(X-\alpha_1^r)\cdots(X-\alpha_n^r)$ are symmetric polynomials in $\alpha_1,\ldots,\alpha_n$ with K-coefficients (in fact the coefficients are just 0, 1, and -1), so these coefficients are polynomials in the elementary symmetric polynomials in the α_i's with K-coefficients. The elementary symmetric polynomials in the α_i's are the coefficients of $f(X)$ (up to sign), so they lie in K. Therefore any polynomial in the elementary symmetric polynomials in the α_i's with K-coefficients has its coefficients in K. □

Example 18. Let $f(X) = X^2+5X+2 = (X-\alpha)(X-\beta)$ where $\alpha = (-5+\sqrt{17})/2$ and $\beta = (-5-\sqrt{17})/2$. Although α and β are not rational, their elementary symmetric polynomials are rational: $s_1 = \alpha+\beta = -5$ and $s_2 = \alpha\beta = 1$. Therefore any symmetric polynomial in α and β with rational coefficients is rational (since it is a polynomial in $\alpha+\beta$ and $\alpha\beta$ with rational coefficients). In particular, $(X-\alpha^r)(X-\beta^r) \in \mathbf{Q}[X]$ for all $r \geq 1$. Taking $r = 2, 3$, and 4, we have

$$\begin{aligned}
(X-\alpha^2)(X-\beta^2) &= X^2-21X+4,\\
(X-\alpha^3)(X-\beta^3) &= X^2+95X+8,\\
(X-\alpha^4)(X-\beta^4) &= X^2-433X+16.
\end{aligned}$$

Example 19. Let α, β, and γ be the three roots of X^3-X-1, so

$$X^3-X-1 = (X-\alpha)(X-\beta)(X-\gamma).$$

The elementary symmetric polynomials in α, β, and γ are all rational, so for every positive integer r, $(X-\alpha^r)(X-\beta^r)(X-\gamma^r)$ has rational coefficients. As explicit examples,

$$\begin{aligned}
(X-\alpha^2)(X-\beta^2)(X-\gamma^2) &= X^3-2X^2+X-1,\\
(X-\alpha^3)(X-\beta^3)(X-\gamma^3) &= X^3-3X^2+2X-1.
\end{aligned}$$

In the proof of Theorem 5, the fact that the coefficients come from a field F is not important; we never had to divide in F. The same proof shows for any commutative ring R that the symmetric polynomials in $R[T_1,\ldots,T_n]$ are $R[s_1,\ldots,s_n]$. (Actually, there is a slight hitch: if R is not a domain then the formula $\operatorname{mdeg}(fg) = \operatorname{mdeg} f + \operatorname{mdeg} g$ is true only as long as the leading coefficients of f and g are both not zero-divisors in R, and that is true for the relevant case of elementary symmetric polynomials $s_1,\ldots,s_n$, whose leading coefficients equal 1.)

Example 20. Taking α and β as in Example 18, their elementary symmetric polynomials are both integers, so any symmetric polynomial in α and β with integral coefficients is an integral polynomial in $\alpha+\beta$ and $\alpha\beta$ with integral coefficients, and thus is an integer. This implies $(X-\alpha^r)(X-\beta^r)$, whose coefficients are $\alpha^r+\beta^r$ and $\alpha^r\beta^r$, has integral coefficients and not just rational coefficients. Examples of this for small r are seen in Example 18.