SYMMETRIC POLYNOMIALS

KEITH CONRAD

Let F be a field. A polynomial $f(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$ is called *symmetric* if it is unchanged by any permutation of its variables:

$$f(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$$

for every permutation σ of $\{1, \ldots, n\}$.

Example 1. The sum $X_1 + \cdots + X_n$ and product $X_1 \cdots X_n$ are symmetric, as are the power sums $X_1^r + \cdots + X_n^r$ for any $r \geq 1$.

Example 2. Let $f(X_1, X_2, X_3) = X_1^5 + X_2X_3$. This polynomial is unchanged if we interchange X_2 and X_3, but if we interchange X_1 and X_3 then f becomes $X_3^5 + X_2X_1$, which is not f. This polynomial is only "partially symmetric."

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

$$(T - X_1)(T - X_2) \cdots (T - X_n) = T^n - s_1T^{n-1} + s_2T^{n-2} - \cdots + (-1)^n s_n. \tag{1}$$

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

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

is the sum of the products of the X_i's taken k terms at a time. The s_k's are all symmetric in $X_1, \ldots, X_n$ and are called the *elementary* symmetric polynomials – or elementary symmetric functions – in the X_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 $T^3 - T - 1$, so

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

Multiplying out the right side and equating coefficients on both sides, the elementary symmetric functions of 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 $F[X_1, \ldots, X_n]$ 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 multidegree 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 $\mathbf{a} \neq (0, 0, \ldots, 0)$.) This way of ordering n-tuples is called the lexicographic (*i.e.*, dictionary) ordering since it resembles the way words are ordered in the dictionary: first order by the first letter, and for words with the same first letter order by the second letter, and so on.

It is simple to check that for $\mathbf{i}$, $\mathbf{j}$, and $\mathbf{k}$ in $\mathbf{N}^n$,

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

A polynomial $f \in F[X_1, \ldots, X_n]$ can be written in the form

$$f(X_1, \ldots, X_n) = \sum_{i_1, \ldots, i_n} c_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n}.$$

We will abbreviate this in multi-index form to $f = \sum_{\mathbf{i}} c_{\mathbf{i}} T^{\mathbf{i}}$, where $T^{\mathbf{i}} := X_1^{i_1} \cdots X_n^{i_n}$ 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 $f \in F[X_1, \ldots, X_n]$, write $f = \sum_{\mathbf{i}} c_{\mathbf{i}} T^{\mathbf{i}}$. Set the *multidegree* of f to be

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

The multidegree 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. $\operatorname{mdeg}(7X_1X_2^5 + 3X_2) = (1, 5)$ and $\operatorname{lead}(7X_1X_2^5 + 3X_2) = 7$.

Example 11. $\operatorname{mdeg}(X_1) = (1, 0, \ldots, 0)$ and $\operatorname{mdeg}(X_n) = (0, 0, \ldots, 1)$.

Example 12. The multidegrees of the elementary symmetric polynomials are $\operatorname{mdeg}(s_1) = (1, 0, 0, \ldots, 0)$, $\operatorname{mdeg}(s_2) = (1, 1, 0, \ldots, 0), \ldots,$ and $\operatorname{mdeg}(s_n) = (1, 1, 1, \ldots, 1)$. For $k = 1, \ldots, n$, the leading term of s_k is $X_1 \cdots X_k$, 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.*, $X_1X_2^3 + X_1^2$ has degree 4. This degree has values in $\mathbf{N}$ rather than $\mathbf{N}^n$. We won't be using it; the multidegree is more convenient for our purposes.

Our definition of multidegree is specific to calling X_1 the "first" variable and X_n the "last" variable. Despite its *ad hoc* nature (there is nothing intrinsic about making X_1 the "first" variable), the multidegree is useful since it permits us to prove theorems about all multivariable polynomials by induction on the multidegree.

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

Lemma 15. *For nonzero f and g in $F[X_1, \ldots, X_n]$, $\operatorname{mdeg}(fg) = \operatorname{mdeg}(f) + \operatorname{mdeg}(g)$ in $\mathbf{N}^n$ and $\operatorname{lead}(fg) = (\operatorname{lead} f)(\operatorname{lead} g)$.*

For f and g in $F[X_1, \ldots, X_n]$, $\operatorname{mdeg}(f+g) \leq \max(\operatorname{mdeg} f, \operatorname{mdeg} g)$ 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 $g = c'_{\mathbf{b}} T^{\mathbf{b}} + \sum_{\mathbf{j}<\mathbf{b}} c'_{\mathbf{j}} T^{\mathbf{j}}$ with $c'_{\mathbf{b}} \neq 0$. This amounts to pulling out the top multidegree terms of f and g. Then fg has a nonzero term $c_{\mathbf{a}} c'_{\mathbf{b}} T^{\mathbf{a}+\mathbf{b}}$ and every other term has multidegree $\mathbf{a}+\mathbf{j}$, $\mathbf{b}+\mathbf{i}$, or $\mathbf{i}+\mathbf{j}$ where $\mathbf{i} < \mathbf{a}$ and $\mathbf{j} < \mathbf{b}$. By (2), all these other multidegrees are less than $\mathbf{a}+\mathbf{b}$, so $\operatorname{mdeg}(fg) = \mathbf{a}+\mathbf{b} = \operatorname{mdeg} f + \operatorname{mdeg} g$ and $\operatorname{lead}(fg) = c_{\mathbf{a}} c'_{\mathbf{b}} = (\operatorname{lead} f)(\operatorname{lead} g)$. ☐

Now we are ready to prove Theorem 5.

Proof. We want to show every symmetric polynomial in $F[X_1, \ldots, X_n]$ 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 in $F[X_1, \ldots, X_n]$ with multidegree $(0, 0, \ldots, 0)$ is in F, and $F \subset F[s_1, \ldots, s_n]$.

Now pick an $\mathbf{d} \neq (0, 0, \ldots, 0)$ in $\mathbf{N}^n$ and suppose the theorem is proved for all symmetric polynomials with multidegree less than $\mathbf{d}$. Write $\mathbf{d} = (d_1, \ldots, d_n)$. Pick any symmetric polynomial f with multidegree $\mathbf{d}$. (If there aren't any symmetric polynomials with multidegree $\mathbf{d}$, 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:

$$f = c_{\mathbf{d}} X_1^{d_1} \cdots X_n^{d_n} + \sum_{\mathbf{i}<\mathbf{d}} c_{\mathbf{i}} T^{\mathbf{i}}, \tag{3}$$

where $c_{\mathbf{d}} \neq 0$. 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 multidegree than $\mathbf{d}$, 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 $\mathbf{d}$, we must set

$$a_1 = d_1 - d_2, \quad a_2 = d_2 - d_3, \quad \ldots, \quad a_{n-1} = d_{n-1} - d_n, \quad a_n = d_n. \tag{4}$$

But does this make sense? That is, do we know that $d_1 - d_2, d_2 - d_3, \ldots, d_{n-1} - d_n, d_n$ are all nonnegative? If that isn't true then we have a problem. So we need to show the coordinates in $\mathbf{d}$ satisfy

$$d_1 \geq d_2 \geq \cdots \geq d_n \geq 0. \tag{5}$$

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

To appreciate this issue, consider $f = X_1 X_2^5 + 3X_2$. The multidegree 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 $f = X_1 X_2^5 + X_1^5 X_2$ then f is symmetric and $\operatorname{mdeg} f = (5, 1)$ does satisfy (5). The verification of (5) will depend crucially on f being symmetric.

Since $(d_1, \dots, d_n)$ is the multidegree of a nonzero monomial in f, and f is symmetric, every vector with the d_i's permuted is *also* a multidegree of a nonzero monomial in f. (Here is where the symmetry of f in the X_i's is used: under any permutation of the X_i's, f stays unchanged.) Since $(d_1, \dots, d_n)$ is the largest multidegree of all the monomials in f, $(d_1, \dots, d_n)$ must be larger in $\mathbf{N}^n$ than any of its nontrivial permutations[1], which means

$$d_1 \geq d_2 \geq \cdots \geq d_n \geq 0.$$

That shows the definition of $a_1, \dots, a_n$ 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,

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

Therefore f and $c_{\mathbf{d}} s_1^{a_1} \cdots s_n^{a_n}$, where $c_{\mathbf{d}} = \operatorname{lead} f$, have the same leading term, namely $c_{\mathbf{d}} X_1^{d_1} \cdots X_n^{d_n}$. If $f = c_{\mathbf{d}} s_1^{a_1} \cdots s_n^{a_n}$ then we're done. If $f \neq c_{\mathbf{d}} s_1^{a_1} \cdots s_n^{a_n}$ then the difference $f - c_{\mathbf{d}} s_1^{a_1} \cdots s_n^{a_n}$ is nonzero with

$$\operatorname{mdeg}(f - c_{\mathbf{d}} s_1^{a_1} \cdots s_n^{a_n}) < (d_1, \dots, d_n).$$

The polynomial $f - c_{\mathbf{d}} s_1^{a_1} \cdots s_n^{a_n}$ is symmetric since both terms in the difference are symmetric. By induction on the multidegree, $f - c_{\mathbf{d}} s_1^{a_1} \cdots s_n^{a_n} \in F[s_1, \dots, s_n]$, so $f \in F[s_1, \dots, s_n]$. □

Let's summarize the recursive step: if f is a symmetric polynomial in $X_1, \dots, X_n$ then

$$\text{leading term of } f \text{ is } c_{\mathbf{d}} X_1^{d_1} \cdots X_{n-1}^{d_{n-1}} X_n^{d_n} \Longrightarrow \operatorname{mdeg}(f - c_{\mathbf{d}} s_1^{d_1-d_2} \cdots s_{n-1}^{d_{n-1}-d_n} s_n^{d_n}) < \operatorname{mdeg}(f).$$

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, which are

$$s_1 = X + Y + Z, \quad s_2 = XY + XZ + YZ, \quad s_3 = XYZ.$$

Treating X, Y, Z as X_1, X_2, X_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:

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

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 $4s_1s_3$:

$$f - s_1^4 + 4s_1^2 s_2 - 2s_2^2 - 4s_1 s_3 = 0.$$

Thus

$$X^4 + Y^4 + Z^4 = s_1^4 - 4s_1^2 s_2 + 2s_2^2 + 4s_1 s_3. \tag{6}$$

---

[1] A trivial permutation is one that exchanges equal coordinates, like $(2, 2, 1)$ and $(2, 2, 1)$.

Remark 17. The proof we have given here is based on [2, Sect. 7.1], where there is an additional argument that shows the representation of a symmetric polynomial as a polynomial in the elementary symmetric polynomials is unique. (For example, the only expression of $X^4 + Y^4 + Z^4$ as a polynomial in s_1, s_2, and s_3 is the one appearing in (6).) For a different proof of Theorem 5, which uses the more usual notion of degree of a multivariable polynomial described in Remark 14, see [1, Sect. 16.1] (there is a gap in that proof, but the basic ideas are there).

Corollary 18. *Let L/K be a field extension and $f(T) \in K[T]$ factor as*

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

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

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

Proof. The coefficients of $(T - \alpha_1^r)(T - \alpha_2^r) \cdots (T - \alpha_n^r)$ are symmetric polynomials in $\alpha_1, \ldots, \alpha_n$ with coefficients in K, so these coefficients are polynomials in the elementary symmetric polynomials in the α_i's with coefficients in K. The elementary symmetric polynomials in the α_i's are (up to sign) the coefficients of $f(T)$, so they lie in K. Therefore any polynomial in the elementary symmetric functions of the α_i's with coefficients in K lies in K. □

Example 19. Let $f(T) = T^2 + 5T + 2 = (T - \alpha)(T - \beta)$ where $\alpha = (-5 + \sqrt{17})/2$ and $\beta = (-5 - \sqrt{17})/2$. Although α and β are not rational, their elementary symmetric functions 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, $(T - \alpha^r)(T - \beta^r) \in \mathbf{Q}[T]$ for all $r \geq 1$. Taking $r = 2, 3$, and 4, we have

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

Example 20. Let α, β, and γ be the three roots of $T^3 - T - 1$, so

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

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

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

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 $R[X_1, \ldots, X_n]$ 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 21. Taking α and β as in Example 19, their elementary symmetric functions 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 $(T - \alpha^r)(T - \beta^r)$, 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 19.

References

[1] M. Artin, “Algebra,” 2nd ed., Prentice-Hall, 2010.
[2] D. Cox, J. Little, D. O’Shea, “Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra,” Springer-Verlag, New York, 1992.