THE TEACHING OF MATHEMATICS

2012, Vol. XV, 1, pp. 55–59

THE FUNDAMENTAL THEOREM ON SYMMETRIC POLYNOMIALS

Hamza Elhadi S. Daoub

Abstract. In this work we are going to extend the proof of Newton's theorem of symmetric polynomials, by considering any monomial order $>$ on polynomials in n variables $x_1, x_2, \dots, x_n$ over a field k, where the original proof is based on the graded lexicographic order. We will introduce some basic definitions and propositions to support the extended proof.

ZDM Subject Classification: H25; *AMS Subject Classification*: 97H20.

Key words and phrases: Symmetric polynomials.

The fundamental theorem of symmetric polynomials is, as its name suggests, a key result in the subject of root identities. The theorem states that any symmetric polynomial can be represented in terms of the elementary symmetric polynomials. Newton had made an extensive study of symmetric root polynomials as early as the mid-1660s, and was very likely aware of the fundamental theorem at that time. Edwards adds "It must be admitted, however, that neither a careful statement nor a proof of it seems to have been published before the nineteenth century. Everyone seemed familiar with it and used it without inhibition." Kline credits Vandermonde with the first published proof of the fundamental theorem in 1771. However, it should be noted that Vandermonde's version of the result was stated in terms of roots and coefficients of a polynomial. Edwards makes the point that the fundamental theorem is properly about symmetric polynomials in n variables, independent of the context of coefficients and roots of a polynomial. Such a formulation sidesteps any philosophical issues concerning the existence or nature of roots.

Definition 1.1. A polynomial $f \in k[x_1, x_2, \dots, x_n]$ is symmetric if

$$f(x_{\tau(1)}, x_{\tau(2)}, \dots, x_{\tau(n)}) = f(x_1, x_2, \dots, x_n)$$

for every possible permutation $x_{\tau(1)}, x_{\tau(2)}, \dots, x_{\tau(n)}$ of the variables $x_1, x_2, \dots, x_n$.

Definition 1.2. Given variables $x_1, x_2, \dots, x_n$, we define $\sigma_1, \sigma_2, \dots, \sigma_n \in$

$k[x_1, x_2, \dots, x_n]$ by

$$\begin{aligned}
\sigma_1 &= x_1 + x_2 + \cdots + x_n \\
&\dots \\
\sigma_r &= \sum_{\tau(1)<\tau(2)<\cdots<\tau(r)} x_{\tau(1)} x_{\tau(2)} \cdots x_{\tau(r)} \\
&\dots \\
\sigma_n &= x_1 x_2 \cdots x_n
\end{aligned}$$

And σ_i is a symmetric polynomial for all $i = 1, \dots, n$.

Definition 1.3. A monomial ordering on $k[x_1, x_2, \dots, x_n]$ is any relation $>$ on $Z^n_{\geq 0}$, or equivalently, any relation on the set of monomials $x^\alpha, \alpha \in Z^n_{\geq 0}$ satisfying:

i. $>$ is a total ordering on $Z^n_{\geq 0}$.

ii. If $\alpha > \beta$ and $\gamma \in Z^n_{\geq 0}$, then $\alpha + \gamma > \beta + \gamma$.

iii. $>$ is well-ordering on $Z^n_{\geq 0}$. This means that every non-empty subset of $Z^n_{\geq 0}$ has a smallest element under $>$.

Proposition 1.4. *An order relation $>$ on $Z^n_{\geq 0}$ is a well-ordering if and only if every strictly decreasing sequence in $Z^n_{\geq 0}$*

$$\alpha(1) > \alpha(2) > \alpha(3) > \cdots$$

eventually terminates.

Definition 1.5. Let $f = \sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $k[x_1, x_2, \dots, x_n]$ and let $>$ be a monomial order.

The multidegree of f is $multideg(f) = max(\alpha \in Z^n_{\geq 0} : a_\alpha \neq 0)$.

The leading coefficient of f is $LC(f) = a_{multideg(f)} \in k$.

The leading monomial of f is $LM(f) = x^{multideg(f)}$.

The leading term of f is $LT(f) = LC(f) \cdot LM(f)$.

Proposition 1.6. *For $f(x_1, x_2, \dots, x_n)$, $g(x_1, x_2, \dots, x_n) \in k[x_1, x_2, \dots, x_n]$ we have*

$$LT(fg) = LT(f)LT(g).$$

Let $>$ be any monomial order of the variables $x_1, x_2, \dots, x_n$ such that

$$x_{\tau(1)} > x_{\tau(2)} > \cdots > x_{\tau(n)}.$$

According to the Definition 1.3, we notice that

$$\begin{aligned}
x_{\tau(1)} x_{\tau(2)} &> x_{\tau(1)} x_{\tau(i)}, \text{ where } i = 3, \dots, n \\
x_{\tau(1)} x_{\tau(2)} x_{\tau(3)} &> x_{\tau(1)} x_{\tau(2)} x_{\tau(i)}, \text{ where } i = 4, \dots, n
\end{aligned}$$

and so on. The leading term of σ_i is defined as follows:

$$\begin{aligned} LT(\sigma_1) &= x_{\tau(1)} \\ LT(\sigma_2) &= x_{\tau(1)}x_{\tau(2)} \\ &\cdots \\ LT(\sigma_n) &= x_{\tau(1)}x_{\tau(2)}\cdots x_{\tau(n)} \end{aligned}$$

Now, suppose that $f \in k[x_1, x_2, \ldots, x_n]$ be any nonzero symmetric polynomial, and $c_1x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$ be a leading term of f. Consider $g = \sigma_1^{\alpha_1}\sigma_2^{\alpha_2}\cdots\sigma_n^{\alpha_n}$. According to Proposition 1.6, the leading term of g is defined as follows:

$$\begin{aligned} LT(g) &= LT(\sigma_1^{\alpha_1}\sigma_2^{\alpha_2}\cdots\sigma_n^{\alpha_n}) \\ &= LT(\sigma_1^{\alpha_1})LT(\sigma_2^{\alpha_2})\cdots LT(\sigma_n^{\alpha_n}) \\ &= (x_{\tau(1)})^{\alpha_1}(x_{\tau(1)}x_{\tau(2)})^{\alpha_2}\ldots(x_{\tau(1)}x_{\tau(2)}\cdots x_{\tau(n)})^{\alpha_n} \\ &= x_{\tau(1)}^{\alpha_1+\alpha_2+\cdots+\alpha_n}x_{\tau(2)}^{\alpha_2+\cdots+\alpha_n}\cdots x_{\tau(n)}^{\alpha_n} \end{aligned}$$

Therefore, we can find the values of α_i, where

$$\begin{aligned} LT(f) = LT(cg) &\Leftrightarrow c_1x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n} = c_1x_{\tau(1)}^{\alpha_1+\alpha_2+\cdots+\alpha_n}x_{\tau(2)}^{\alpha_2+\ldots\alpha_n}\cdots x_{\tau(n)}^{\alpha_n} \\ &\Leftrightarrow a_{\tau(1)} = \alpha_1+\alpha_2+\cdots+\alpha_n \\ &\text{and } a_{\tau(2)} = \alpha_2+\alpha_3+\cdots+\alpha_n \\ &\ldots \\ &\text{and } a_{\tau(n)} = \alpha_n \end{aligned}$$

Thus,

$$\begin{aligned} \alpha_n &= a_{\tau(n)} \\ \alpha_{n-1} &= a_{\tau(n-1)} - a_{\tau(n)} \\ \alpha_{n-2} &= a_{\tau(n-2)} - a_{\tau(n-1)} \\ &\cdots \\ \alpha_2 &= a_{\tau(2)} - a_{\tau(3)} \\ \alpha_1 &= a_{\tau(1)} - a_{\tau(2)} \end{aligned}$$

Then, the map

$$(a_1, a_2, \ldots, a_n) \mapsto (a_{\tau(1)} - a_{\tau(2)}, a_{\tau(2)} - a_{\tau(3)}, \ldots, a_{\tau(n-1)} - a_{\tau(n)}, a_{\tau(n)})$$

defines the relation between the leading terms of f and g.

Theorem 1.7. [Newton's Theorem] *Any symmetric polynomial in $k[x_1, x_2, \ldots, x_n]$ can be written as a polynomial in $\sigma_1, \sigma_2, \ldots, \sigma_n$ with coefficients in k and this polynomial is unique.*

Proof. We will follow the argument above. So let $>$ be any monomial ordering of the variables $x_1, x_2, \ldots, x_n$ such that.

$$x_{\tau(1)} > x_{\tau(2)} > \cdots > x_{\tau(n)}$$

Let $c_1 x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ be a leading term of f, and consider

$$\begin{aligned} g &= \sigma_1^{a_{\tau(1)}-a_{\tau(2)}} \sigma_2^{a_{\tau(2)}-a_{\tau(3)}} \cdots \sigma_n^{a_{\tau(n)}}. \\ LT(c_1 g) &= LT(c_1 \sigma_1^{a_{\tau(1)}-a_{\tau(2)}} \sigma_2^{a_{\tau(2)}-a_{\tau(3)}} \cdots \sigma_n^{a_{\tau(n)}}) \\ &= c_1 (x_{\tau(1)})^{a_{\tau(1)}-a_{\tau(2)}} (x_{\tau(1)} x_{\tau(2)})^{a_{\tau(2)}-a_{\tau(3)}} \cdots (x_{\tau(1)} x_{\tau(2)} \cdots x_{\tau(n)})^{a_{\tau(n)}} \\ &= c_1 x_{\tau(1)}^{a_{\tau(1)}} x_{\tau(2)}^{a_{\tau(2)}} \cdots x_{\tau(n)}^{a_{\tau(n)}} \\ &= LT(f) \end{aligned}$$

for any permutation τ. This shows that f and $c_1 g$ have the same leading term. Hence $f_1 = f - c_1 g$ has a strictly smaller leading term according to the monomial ordering, which is defined above. Since f and g are symmetric polynomials, then so is f_1.

Now we repeat this process, starting with f_1 instead of f, where f_1 has a leading term with coefficient c_2 and exponent $b_1 < b_2 < \cdots < b_n$. As above, there is a symmetric polynomial g_1 such that f_1 and $c_2\ g_1$ have the same leading term. It follows that

$$f_2 = f_1 - c_2 g_1 = f - c_1 g - c_2 g_1$$

has a strictly smaller leading term. Continuing in this way, we get polynomials:

$$f, f_1 = f - c_1 g, f_2 = f - c_1 g - c_2 g_1, f_3 = f - c_1 g - c_2 g_1 - c_3 g_1, \ldots$$

where at each stage the leading term gets smaller according to the ordering monomial. This process will terminate when we find some m with $f_m = 0$; if not, then the above would give an infinite sequence of nonzero polynomials with strictly decreasing leading term, which contradicts Proposition 1.4. Hence, this process must terminate.

Once we have $f_m = 0$ for some m, we obtain

$$f = c_1 g + c_2 g_1 + \cdots + c_m g_{m-1}$$

where each g_i is a product of the σ_i to various powers, which proves that f is a polynomial in the elementary symmetric polynomials.

To prove the uniqueness, suppose that $k[y_1, y_2, \ldots, y_n]$ be a polynomial ring with new variables $y_1, y_2, \ldots, y_n$. Since the evaluation map which sends y_i to $\sigma_i \in k[x_1, x_2, \ldots, x_n]$ defines a ring homomorphism

$$\varphi : k[y_1, y_2, \ldots, y_n] \to k[x_1, x_2, \ldots, x_n]$$

Then, if $g = g(y_1, y_2, \ldots, y_n) \in k[y_1, y_2, \ldots, y_n]$, we get

$$\varphi(g) = g(\sigma_1, \sigma_2, \ldots, \sigma_n)$$

Recall that the set of all polynomials in the σ_i with coefficient in k is a subring of $k[x_1, x_2, \ldots, x_n]$, so we can write φ as a map

$$\varphi : k[y_1, y_2, \ldots, y_n] \to k[\sigma_1, \sigma_2, \ldots, \sigma_n]$$

where $k[\sigma_1, \sigma_2, \ldots, \sigma_n]$ is the set of all polynomials in σ_i with coefficients in k.

The last map is onto by the definition. To prove the uniqueness we need to prove that φ is one to one. It is sufficient to show that $ker\varphi = 0$, which means for any nonzero polynomial g in y_i, then $g(\sigma_1, \sigma_2, \ldots, \sigma_n) \neq 0$.

Let $cu_1^{b_1} u_2^{b_2} \cdots u_n^{b_n}$ be any nonzero term in g. Applying φ gives $g = \sigma_1^{b_1} \sigma_2^{b_2} \cdots \sigma_n^{b_n}$. As we mentioned before the theorem, the leading term of $g = \sigma_1^{\alpha_1} \sigma_2^{\alpha_2} \cdots \sigma_n^{\alpha_n}$ is

$$cx_{\tau(1)}^{b_1+b_2+\cdots+b_n} x_{\tau(2)}^{b_2+\cdots+b_n} \cdots x_{\tau(n)}^{b_n}.$$

Since g is the sum of its terms, so the corresponding polynomial $\varphi(g)$ is sum of $c\sigma_1^{b_1} \sigma_2^{b_2} \cdots \sigma_n^{b_n}$.

The crucial fact is that the map

$$(b_{\tau(1)}, b_{\tau(2)}, \ldots, b_{\tau(n)}) \mapsto (b_1 + b_2 + \cdots + b_n, b_2 + \cdots + b_n, \ldots, b_n)$$

is one to one, so the leading terms cannot all cancel, and $\varphi(g)$ cannot be the zero-polynomial. Hence the uniqueness follows. ■

REFERENCES

[1] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer Verlag UTM, New York, 1992.

[2] D. A.Cox, *Galois Theory*, John Wiley and Sons, INC., New Jersey, 2004.

[3] D. Kalman, *Uncommon Mathematical Excursions, Polynomia and Related Realms*, The Mathematical Association of America, Number 35, 2009.

Faculty of Mathematics, University of Belgrade, Serbia