An inductive proof of Newton's identities

by Zinovy Reichstein

Let $f(x) = x^n + s_1 x^{n-1} + \ldots + s_{n-1}x + s_n$ be a monic polynomial and let $x_1, \ldots, x_n$ be the roots of f. Expanding the product

$$f(x) = (x - x_1) \ldots (x - x_n) \ ,$$

we find that

$$s_r = (-1)^r \sum_{i_1 < \ldots < i_i} x_{i_1} \ldots x_{i_r} \ .$$

The expressions s_r may be viewed as polynomials in $x_1, \ldots, x_n$; they play an important role in algebra, combinatorics, and many other areas of mathematics. Note that each s_r is symmetric (i.e., it does not change if we permute $x_1, \ldots, x_n$) and homogeneous of degree r. These polynomials, often called elementary symmetric polynomials[1], form a "basis" for all symmetric polynomials in the sense that every symmetric polynomial in $x_1, \ldots, x_n$ can be uniquely written as a polynomial in $s_1, \ldots, s_n$.

Another important family of symmetric polynomials is given by

$$p_r(x_1, \ldots, x_n) = x_1^r + \ldots + x_n^r \ .$$

In fact, $p_1, \ldots, p_n$ also form a basis for the space of all symmetric polynomials (with rational, real or complex coefficients)[2].

The transition formulas between these two bases are known as "Newton's formulas" or "Newton's identities"; they first appeared Newton's book *Arithmetica universalis* written between 1673 and 1683. If we set $s_{n+1} = s_{n+2} = \ldots = 0$ then we can write them as

$$p_d + s_1 p_{d-1} + \ldots + s_{d-1} p_1 + d p_0 = 0. \tag{1}$$

Note that (1) is, in fact, a family of identities, depending on n and d, where n and d are allowed to range over the natural numbers.

[1]More precisely, the term "the rth elementary symmetric polynomial" usually refers to $(-1)^r s_r$.

[2]In applications of algebra to coding theory, one usually considers polynomials whose coefficients lie in a finite field. In this case $s_1, \ldots, s_n$ still form a basis for all symmetric polynomials but $p_1, \ldots, p_n$ will not do so in general. Newton's formulas turn out to be very helpful in this setting; see, e.g., [1].

A number of proofs of Newton's identities has appeared in the literature over the years, and new proofs continue to be published; see, e.g., [2], [3]. In this note we offer yet another proof. Denote the left hand side of (1) by $F_n^{(d)}$. Our goal is to show that $F_n^{(d)}(x_1,\ldots,x_n)=0$ for every $n,d\in\mathbf{N}$. The proof proceeds by induction on $m=n-d$.

Since $m=n-d$ may take on any integer value, positive or negative, the base case of our argument will cover the entire range $m\le 0$, i.e., $d\ge n$. Indeed, from the definition of $s_1,\ldots,s_n$, we see that

$$\begin{aligned} f(x_1) &= x_1^n+s_1x_1^{n-1}+\ldots+s_n=0\ , \\ &\vdots \\ f(x_n) &= x_n^n+s_1x_n^{n-1}+\ldots+s_n=0 \end{aligned}$$

Adding these equations together, we obtain

$$p_n+s_1p_{n-1}+\ldots++s_{n-1}p_1+ns_n=0\ .$$

or equivalently, $F_n^{(n)}=0$. Similarly, expanding

$$x_1^{d-n}f(x_1)+\ldots+x_n^{n-d}f(x_n)=0\ ,$$

we conclude that $F_n^{(d)}=0$ for any $d\ge n$.

We are now ready to perform the induction step. Choose n and $d\in\mathbf{N}$ so that $m=n-d\ge 1$. Assume that $F_{n'}^{(d')}=0$ whenever $n'-d'\le m-1$. We want to show that $F_n^{(d)}=0$. First note that

$$F_n^{(d)}(x_1,\ldots,x_{n-1},0)=F_{n-1}^{(d)}(x_1,\ldots,x_{n-1})\ .$$

(This follows from our definition of s_r and p_r; please check!) By the induction assumption $F_{n-1}^{(d)}(x_1,\ldots,x_{n-1})=0$. This means that $F_n^{(d)}$ is divisible by x_n. Since $F_n^{(d)}$ is a symmetric polynomial, it is also divisible by $x_1,\ldots,x_{n-1}$, i.e., $F_n^{(d)}$ is divisible by $x_1\ldots x_n$. On the other hand, note that $F_n^{(d)}$ is a homogeneous polynomial of degree $d<n$; if it is nonzero, it cannot be divisible by $x_1\ldots x_n$. Thus $F_n^{(d)}=0$, as claimed.

References

[1] Berlekamp, E., Algebraic Coding Theory, McGraw-Hill, New York, 1968. Russian translation: Algebraicheskaya teoriya kodirovaniya, translated by I. I. Grishko, edited by S. D. Berman, Mir Publishers, Moscow, 1971.

[2] Meed, D. G., *Newton's indentities*, American Math. Monthly **99**, no. 8 (1992), pp. 749–751.

[3] Zeidelberg, D., *A combinatorial proof of Newton's identities*, Discrete Math. **49**, no. 3 (1984), p. 319.