ON RESULTANTS

GERALD MYERSON

Abstract. Let $f$ and $g$ be polynomials with coefficients in a commutative ring $A$. Let $f$ be monic. We show that the resultant of $f$ and $g$ equals the norm from $A[x]/(f)$ to $A$ of $\bar{g}$. As a corollary we deduce that if $c$ is in $A$ and also in the ideal generated by $f$ and $g$, then the resultant divides $c^n$, where $n$ is the degree of $f$.

In this paper $A$ will denote a commutative ring with unity. Let $f$ be a monic polynomial with coefficients in $A$. Let $P = A[x]/(f)$. Given $\alpha$ in $B$ the norm of $\alpha$, denoted $N(\alpha)$, is defined to be the determinant of the right regular representation of $\alpha$.

Now let $f(x) = \sum_{j=0}^{n} a_{n-j} x^j$ and $g(x) = \sum_{j=0}^{m} b_{m-j} x^j$ be polynomials with coefficients in $A$. The resultant of $f$ and $g$, denoted $R(f, g)$, is given by:

$$R(f, g) = \det \begin{pmatrix} a_0 & a_1 & \cdots & a_n & 0 \\ a_0 & \cdots & a_n & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & a_0 & \cdots & a_n \\ b_0 & b_1 & \cdots & b_m & 0 \\ b_0 & \cdots & b_m & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots \\ 0 & b_0 & \cdots & b_m & \end{pmatrix}_{m \times m}$$

Theorem. Let $f$ and $g$ be polynomials with coefficients in $A$, $f$ monic. Let $\bar{g}$ be the class of $g$ in $A[x]/(f)$. Then $N(\bar{g}) = R(f, g)$.

Proof. On the hypotheses, the first $m$ terms on the diagonal of the matrix above are ones. Gaussian elimination applied to the matrix, using these elements as pivots, yields $R(f, g) = \det(I_n^0 M)$, where $I$ is the $m \times m$ identity matrix. Thus, $R(f, g) = \det M$. But it is easily checked that $M$ is the transpose of the right regular representation of $\bar{g}$.

Corollary. If $f$, $g$, $r$ and $s$ are polynomials with coefficients in $A$, and $f$ is monic then $R(f, fr + gs) = R(f, g)R(f, s)$.

Received by the editors October 26, 1982 and, in revised form, January 12, 1983.

1980 Mathematics Subject Classification. Primary 13B25, 10M05.

Key words and phrases. Resultants.

©1983 American Mathematical Society

0002-9939/83 $1.00 + $.25 per page

419
Remark. This is well known, at least when $A$ is taken to be a field. The theorem above permits a one-line proof.

Proof. $R(f, fr + gs) = N(fr + gs) = N(gs) = N(\overline{g})N(\overline{s}) = R(f, g)R(f, s)$.

Corollary. Let $f$ and $g$ be as in the Theorem above. Let $J = J(f, g)$ be the ideal generated by $f$ and $g$ in $A[x]$, and let $c$ be an element of $J \cap A$. Then $R(f, g)$ divides $c^n$, where $n$ is the degree of $f$.

Remark. That $R(f, g)$ divides some power of $c$ is known (see e.g. [2, Lemma 11.3]). In transcendence theory it is often helpful to have bounds for a nonzero resultant (see, e.g. [1]). We present the Corollary in the spirit of such bounds.

Proof. Let $f$, $g$ and $c$ be as given. Then there exist polynomials $r$ and $s$ with coefficients in $A$ such that $c = fr + gs$. Then $c^n = R(f, c) = R(f, fr + gs) = R(f, g)R(f, s)$, whence $R(f, g)$ divides $c^n$.

This Corollary is sharp, in the following sense. Given any nonunit $c$ in $A$, and any positive integer $n$, there exist $f$ and $g$ in $A[x]$, $f$ monic of degree $n$, such that $c$ is in $J(f, g)$, and $R(f, g)$ does not divide $c^{n-1}$. For example, take $f(x) = x^n$, $g(x) = x^n + c$; then $R(f, g) = c^n$.

Moreover, it is not possible, in general, to remove the condition that $f$ be monic. Take for $A$ the integers, let $f(x) = 2x + 1$, and let $g(x) = 2x + 17$. Then $1$ is in $J(f, g)$, since

$$x^4g(x) - (x^4 + 8x^3 - 4x^2 + 2x - 1)\overline{f}(x) = 1.$$  

However, $R(f, g) = 32$. The construction exemplified here is clearly quite general.

If it is required that the leading coefficients of $f$ and $g$ be relatively prime, it can be shown that if $c$ is in $A \cap J(f, g)$ then $R(f, g)$ divides $c^k$, where $k = \max(m, n)$.

We note as a further corollary that, under the assumption that $f$ is monic, $J(f, g)$ contains $A$ if and only if $R(f, g)$ is a unit. We would like to propose the problem of characterizing those pairs $f, g$ for which $R(f, g)$ is a unit or, more generally, for which $R(f, g)$ divides every element of $A \cap J(f, g)$.

We would like to acknowledge the helpful comments of the referee and editor, which led us to an extensive revision of our original manuscript.

References


Department of Mathematics, University of British Columbia, Vancouver, British Columbia, Canada V6T 1Y4

Current address: Department of Mathematics, State University of New York at Buffalo, Buffalo, New York 14214-3093