Miskolc Mathematical Notes
Vol. 16 (2015), No 1, pp. 205-211

HU e-ISSN 1787-2413
DOI: 10.18514/MMN.2015.1369

Simple proofs of some theorems in resultant theory

Amir Hashemi and Farzad Mirzavand

Miskolc Mathematical Notes
Vol. 16 (2015), No. 1, pp. 205–211

HU e-ISSN 1787-2413

SIMPLE PROOFS OF SOME THEOREMS IN RESULTANT THEORY

AMIR HASHEMI AND FARZAD MIRZAVAND

Received 10 October, 2014

Abstract. In this note, using elementary results from algebraic geometry, we give new and simple proofs of some known theorems in resultant theory.

2010 *Mathematics Subject Classification:* 13P15

Keywords: homogeneous polynomials, multivariate resultants, three ternary quadrics system

1. INTRODUCTION

The multivariate resultant is a fundamental tool of computational algebraic geometry which was introduced by *F. S. Macaulay* [4] in 1902 after earlier work due to Euler, Sylvester and Cayley. The resultant of a polynomial system has many important properties for the geometry of the variety that the system defines. Indeed, the resultant is an algebraic condition in terms of the coefficients of a given system of polynomials which is satisfied if and only if the system has a common solution. More precisely, suppose that K is an algebraically closed field. Let $f = a_0 + \cdots + a_l x^l$ and $g = b_0 + \cdots + b_m x^m$ be two univariate polynomials where a_i's and b_i's belong to K and $a_l, b_m \neq 0$. The *Sylvester* matrix of f, g is defined as

$$S(f,g) = \begin{bmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & \\ \vdots & a_2 & \ddots & a_0 & \vdots & b_2 & \ddots & b_0 \\ a_l & \vdots & \ddots & a_1 & b_m & \vdots & \ddots & b_1 \\ & a_l & & a_2 & & b_m & & b_2 \\ & & \ddots & \vdots & & & \ddots & \vdots \\ & & & a_l & & & & b_m \end{bmatrix}.$$

The univariate resultant of f and g is the determinant of $S(f,g)$ and is denoted by $\mathrm{Res}(f,g)$. It is well known that $\mathrm{Res}(f,g) = 0$ if and only if f and g have a

nontrivial common root (see [1, Chapter 3, Proposition 1.7]). A generalization of this result can be used to decide whether a system of $n+1$ homogeneous equations in $n+1$ variables has a solution or not. Throughout this note we let $R = K[x_0,\dots,x_n]$. To state the next theorem, we need to introduce some notation. Let $F_0,\dots,F_n \in R$ be $n+1$ homogeneous polynomials of degrees $d_0,\dots,d_n$. So, we can write F_i as $\sum_{|\alpha|=d_i} c_{i,\alpha}x^\alpha$ where some of the $c_{i,\alpha}$'s may be zero. For each possible pair of indices i,α, we introduce a new variable $u_{i,\alpha}$. Let us associate a polynomial $P \in \mathbb{Z}[u_{i,\alpha}]$ to the *universal* homogeneous polynomials $\sum_{|\alpha|=d_i} u_{i,\alpha}x^\alpha$ for $i = 0,\dots,n$. Then, when the polynomial P for a particular collection of polynomials $\sum_{|\alpha|=d_i} c_{i,\alpha}x^\alpha$ for $i = 0,\dots,n$ is considered, for each i and α, the variable $u_{i,\alpha}$ is substituted by $c_{i,\alpha}$ into P.

Theorem 1 ([1, Chapter 3, Theorem 2.3])**.** *Let us fix the degrees $d_0,\dots,d_n$. Then there is a unique polynomial* $\mathrm{Res} \in \mathbb{Z}[u_{i,\alpha}]$ *which has the following properties:*

(1) *If $F_0,\dots,F_n \in R$ are homogeneous of degrees, respectively $d_0,\dots,d_n$, then the system $F_0 = \cdots = F_n = 0$ have a nontrivial solution over K if and only if* $\mathrm{Res}(F_0,\dots,F_n) = 0$,
(2) $\mathrm{Res}(x_0^{d_0},\dots,x_n^{d_n}) = 1$,
(3) Res *is irreducible as a polynomial in* $K[u_{i,\alpha}]$.

If we fix the degrees $d_0,\dots,d_n$, then the polynomial $\mathrm{Res} = \mathrm{Res}_{d_0,\dots,d_n} \in \mathbb{Z}[u_{i,\alpha}]$ is called the *resultant* polynomial corresponding to $d_0,\dots,d_n$. Further, the constant $\mathrm{Res}(F_0,\dots,F_n) \in K$ is called the *resultant* of $F_0,\dots,F_n$. For more details, we refer the reader to the books [1,2,5]. The resultant has many algebraic properties that make it a convenient tool in constructive algebra. In this note, we consider the symmetry and multiplicativity property of resultant.

Theorem 2. *Suppose that $F_0,\dots,F_n \in R$ are homogeneous of degrees, respectively $d_0,\dots,d_n$.*

(*a*) *If $i < j$ then*

$$\mathrm{Res}(F_0,\dots,F_i,\dots,F_j,\dots,F_n) = (-1)^{d_0\cdots d_n}\mathrm{Res}(F_0,\dots,F_j,\dots,F_i,\dots,F_n).$$

(*b*) *If $F_j = F_j'F_j''$ is a product of homogeneous polynomials of degrees d_j' and d_j'' then*

$$\mathrm{Res}(F_0,\dots,F_n) = \mathrm{Res}(F_0,\dots,F_j',\dots,F_n)\mathrm{Res}(F_0,\dots,F_j'',\dots,F_n).$$

In 1991, Jouanolou [3, Section 5], proved this theorem, however, in Section 2 we give a new and elementary proof for it. Further, in Section 3, we use some effective elementary algebraic geometry results to prove the necessary and sufficient conditions for the satisfiability of the "three ternary quadrics" system. For the classical proof of this result, we refer the reader to ([6, Art. 90] and [1, page 88]).

2. THE PROOF OF THEOREM 2

In order to prove this theorem, we need some properties of ideals and varieties. Let $R = K[x_0, \ldots, x_n]$ be a polynomial ring over an algebraically closed field K and $I \subset R$ a homogeneous ideal. Further, let $f_1, \ldots, f_k$ be polynomials (not necessarily homogeneous) in R. Then, the *variety* defined by $f_1, \ldots, f_k$ is the set

$$\mathbf{V}(f_1, \ldots, f_k) = \{(a_0, \ldots, a_n) \in K^{n+1} \mid f_i(a_0, \ldots, a_n) = 0 \text{ for all } i\}.$$

A subset $V \subset K^{n+1}$ is called a variety if there exist $f_1, \ldots, f_k \in R$ so that $V = \mathbf{V}(f_1, \ldots, f_k)$. Further, the ideal of a variety V is defined to be
$\mathbf{I}(V) = \{f \in R \mid f(a_0, \ldots, a_n) = 0 \text{ for all } (a_0, \ldots, a_n) \in V\}$.

Theorem 3 (Hilbert's Nullstellensatz)**.** *Suppose that $I = \langle f_1, \ldots, f_k \rangle$ is the ideal generated by the f_i's. Then, $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_k)) = \sqrt{I}$.*

For more details on this topic we refer the reader to [1, 2].

Theorem 4 ([1, Theorem 3.1, page 95])**.** *Let us fix the degrees $d_0, \ldots, d_n$, then the polynomial $\mathrm{Res}_{d_0,\ldots,d_n}$ has the total degree $\sum_{j=0}^{n} d_0 \cdots d_{j-1} d_{j+1} \cdots d_n$.*

We continue with some notation. Let $F \in R$ be a homogeneous polynomial. Then, we denote the polynomial $F(x_0, \ldots, x_{n-1}, 0)$ and $F(x_0, \ldots, x_{n-1}, 1)$ by $\bar{F}(x_0, \ldots, x_{n-1})$ and $f(x_0, \ldots, x_{n-1})$, respectively.

Theorem 5 ([1, Theorem 3.4, page 96])**.** *If $\mathrm{Res}(\bar{F}_0, \ldots, \bar{F}_{n-1}) \neq 0$, then we have $\mathrm{Res}(F_0, \ldots, F_n) = \mathrm{Res}(\bar{F}_0, \ldots, \bar{F}_{n-1})^{d_n} . \det(m_{f_n})$ where m_{f_n} is the linear multiplication map by f_n on $K[x_0, \ldots, x_{n-1}]/\langle f_0, \ldots, f_{n-1} \rangle$.*

Proof. of Theorem 2: (a) Let us denote by $R_{i,j}$ and $R_{j,i}$ the polynomials $\mathrm{Res}(F_0, \ldots, F_n)$ and $\mathrm{Res}(F_0, \ldots, F_j, \ldots, F_i, \ldots, F_n)$, respectively. By Theorem 1, if $R_{j,i}$ vanishes, then

$$F_0 = \cdots = F_j = \cdots = F_i = \cdots = F_n = 0$$

has a nontrivial solution. On the other hand, every nontrivial solution of this system is a nontrivial solution of $F_0 = \cdots = F_n = 0$. Hence $R_{i,j}$ vanishes on the set $\mathbf{V}(R_{j,i})$. This shows that

$$R_{i,j} \in \mathbf{I}(\mathbf{V}(R_{j,i})) = \sqrt{\langle R_{j,i} \rangle}.$$

However, $R_{j,i}$ is irreducible, which implies that $R_{i,j} \in \langle R_{j,i} \rangle$. By Theorem 4, $R_{i,j}$ and $R_{j,i}$ have the same degree. This follows that there exists a constant c so that $R_{i,j} = c R_{j,i}$. We shall prove that $c = (-1)^{d_0 \cdots d_n}$. Since c is constant, it's enough to show that

$$\mathrm{Res}(x_0^{d_0}, \ldots, x_n^{d_n}) = (-1)^{d_0 \cdots d_n} \mathrm{Res}(x_0^{d_0}, \ldots, x_j^{d_j}, \ldots, x_i^{d_i}, \ldots, x_n^{d_n}).$$

In doing so, we will use induction on the number of polynomials. For $n = 2$, the claim is implied by the main properties of determinants. Now assume that the claim holds

for n polynomials of degrees $d_0,\ldots,d_{n-1}$. By applying Theorem 5 on $x_0^{d_0},\ldots,x_n^{d_n}$ and $x_0^{d_0},\ldots,x_j^{d_j},\ldots,x_i^{d_i},\ldots,x_n^{d_n}$, it follows respectively that

$$\det(m_{x_n^{d_n}}) = \frac{\mathrm{Res}(x_0^{d_0},\ldots,x_n^{d_n})}{\mathrm{Res}(x_0^{d_0},\ldots,x_{n-1}^{d_{n-1}})^{d_n}}$$

$$\det(m_{x_n^{d_n}}) = \frac{\mathrm{Res}(x_0^{d_0},\ldots,x_j^{d_j},\ldots,x_i^{d_i},\ldots,x_n^{d_n})}{\mathrm{Res}(x_0^{d_0},\ldots,x_j^{d_j},\ldots,x_i^{d_i},\ldots,x_{n-1}^{d_{n-1}})^{d_n}}.$$

Thus, we can write

$$\frac{\mathrm{Res}(x_0^{d_0},\ldots,x_n^{d_n})}{\mathrm{Res}(x_0^{d_0},\ldots,x_{n-1}^{d_{n-1}})^{d_n}} = \frac{\mathrm{Res}(x_0^{d_0},\ldots,x_j^{d_j},\ldots,x_i^{d_i},\ldots,x_n^{d_n})}{\mathrm{Res}(x_0^{d_0},\ldots,x_j^{d_j},\ldots,x_i^{d_i},\ldots,x_{n-1}^{d_{n-1}})^{d_n}}$$

and therefore from the induction hypothesis we can conclude that

$$\begin{aligned}
&\frac{\mathrm{Res}(x_0^{d_0},\ldots,x_n^{d_n})}{\frac{\mathrm{Res}(x_0^{d_0},\ldots,x_{n-1}^{d_{n-1}})^{d_n}\cdot\mathrm{Res}(x_0^{d_0},\ldots,x_j^{d_j},\ldots,x_i^{d_i},\ldots,x_n^{d_n})}{\mathrm{Res}(x_0^{d_0},\ldots,x_j^{d_j},\ldots,x_i^{d_i},\ldots,x_{n-1}^{d_{n-1}})^{d_n}}}\\
=\ &\frac{(-1)^{d_0\cdots d_n}\mathrm{Res}(x_0^{d_0},\ldots,x_j^{d_j},\ldots,x_i^{d_i},\ldots,x_{n-1}^{d_{n-1}})^{d_n}\cdot\mathrm{Res}(x_0^{d_0},\ldots,x_j^{d_j},\ldots,x_i^{d_i},\ldots,x_n^{d_n})}{\mathrm{Res}(x_0^{d_0},\ldots,x_j^{d_j},\ldots,x_i^{d_i},\ldots,x_{n-1}^{d_{n-1}})^{d_n}}\\
=\ &(-1)^{d_0\cdots d_n}\mathrm{Res}(x_0^{d_0},\ldots,x_j^{d_j},\ldots,x_i^{d_i},\ldots,x_n^{d_n})
\end{aligned}$$

which proves the assertion. To prove (b), let us denote by R,R',R'' the polynomials $\mathrm{Res}(F_0,\ldots,F_j,\ldots,F_n),\mathrm{Res}(F_0,\ldots,F_j',\ldots,F_n),\mathrm{Res}(F_0,\ldots,F_j'',\ldots,F_n)$. We shall show that $R=R'R''$. Note that R may be considered as a polynomial in the coefficients of $F_0,\ldots,F_j',F_j'',\ldots,F_n$. By Theorem 1, if either R' or R'' vanishes, then either the system $F_0=\cdots=F_j'=\cdots=F_n=0$ or the system $F_0=\cdots=F_j''=\cdots=F_n=0$ has a nontrivial solution. Every nontrivial solution of these systems is a nontrivial solution of the system $F_0=\cdots=F_n=0$. Note that we consider R,R' and R'' as the polynomials in the coefficients of polynomials $F_0,\ldots,F_j',F_j'',\ldots,F_n,$. Then due to the irreducibility of R' and R'', we have

$$R\in\mathbf{I}(\mathbf{V}(R'))=\sqrt{\langle R'\rangle}=\langle R'\rangle,\qquad R\in\mathbf{I}(\mathbf{V}(R''))=\sqrt{\langle R''\rangle}=\langle R''\rangle.$$

This proves that $R'\mid R$ and $R''\mid R$. It should be noted that R' and R have degrees 0 and $d_0\cdots d_{j-1}d_{j+1}\cdots d_n$ in the coefficients of polynomial F_j'', respectively. Also, R' and R have degree $d_0\cdots d_{j-1}d_{j+1}\cdots d_n$ in the coefficients of polynomial F_j'. Thus, there exists a polynomial g such that $R=gR'$ where g has degree 0 and $d_0\cdots d_{j-1}d_{j+1}\cdots d_n$ in the coefficients of F_j' and F_j'', respectively. From $R\in\langle R''\rangle$ it implies that $R''\mid gR'$. On the other hand, R'' is irreducible, which implies that R'' divides either g or R'. Since R' and R'' have degrees 0 and $d_0\cdots d_{j-1}d_{j+1}\cdots d_n$ in

the coefficients of F_j'', it follows that $R'' \mid g$. Since R'' and g have the same degree in the coefficients of polynomial F_j'' there exists a polynomial c of degree 0 in the coefficients of F_j'' such that $g = cR''$. Thus, we conclude that $R = cR'R''$. Note that R and $R'R''$ have the same total degree. Therefore c is constant. From the equality

$$F_0 = x_0^{d_0}, \ldots, F_j' = x_j^{d_j'}, F_j'' = x_j^{d_j''}, \ldots, F_n = x_n^{d_n},$$

we see that $R = R' = R'' = 1$ and thus $c = 1$, which implies that $R = R'R''$ and this ends the proof. □

3. THREE TERNARY QUADRICS SYSTEM

In this section we consider the classical system of three ternary quadrics. This is the following system

$$\begin{array}{lllllllllllll} F_0 = c_{01}x^2 & + & c_{02}y^2 & + & c_{03}z^2 & + & c_{04}xy & + & c_{05}xz & + & c_{06}yz = 0 \\ F_1 = c_{11}x^2 & + & c_{12}y^2 & + & c_{13}z^2 & + & c_{14}xy & + & c_{15}xz & + & c_{16}yz = 0 \\ F_2 = c_{21}x^2 & + & c_{22}y^2 & + & c_{23}z^2 & + & c_{24}xy & + & c_{25}xz & + & c_{26}yz = 0 \end{array}$$

where the c_{ij}'s are parameters. By Theorem 1, $\mathrm{Res}(F_0, F_1, F_2)$ vanishes exactly when this system has a nontrivial solution in x, y and z. However, $\mathrm{Res}(F_0, f_1, F_2)$ is a large polynomial in 18 variables with 21894 terms (see [1, page 88]). The aim of this section is to provide a new and simple proof for a compact representation of $\mathrm{Res}(F_0, F_1, F_2)$. For the original proof, we refer to [6, Art. 90]. Let us denote by J the Jacobian determinant of F_0, F_1, F_2 w.r.t. the variables x, y and z. Then, the partial derivatives of J are quadratic and hence we can write

$$\begin{array}{lllllllllllll} \frac{\partial J}{\partial x} & = & b_{01}x^2 & + & b_{02}y^2 & + & b_{03}z^2 & + & b_{04}xy & + & b_{05}xz & + & b_{06}yz \\ \frac{\partial J}{\partial y} & = & b_{11}x^2 & + & b_{12}y^2 & + & b_{13}z^2 & + & b_{14}xy & + & b_{15}xz & + & b_{16}yz \\ \frac{\partial J}{\partial z} & = & b_{21}x^2 & + & b_{22}y^2 & + & b_{23}z^2 & + & b_{24}xy & + & b_{25}xz & + & b_{26}yz. \end{array}$$

Proposition 1.

$$\mathrm{Res}(F_0, F_1, F_2) = \frac{-1}{512} \det \begin{bmatrix} c_{01} & c_{02} & c_{03} & c_{04} & c_{05} & c_{06} \\ c_{11} & c_{12} & c_{13} & c_{14} & c_{15} & c_{16} \\ c_{21} & c_{22} & c_{23} & c_{24} & c_{25} & c_{26} \\ b_{01} & b_{02} & b_{03} & b_{04} & b_{05} & b_{06} \\ b_{11} & b_{12} & b_{13} & b_{14} & b_{15} & b_{16} \\ b_{21} & b_{22} & b_{23} & b_{24} & b_{25} & b_{26} \end{bmatrix}.$$

Proof. We refer to the right hand side matrix as A. If we regard the monomials $x^2, y^2, z^2, xy, xz, yz$ as unknowns, then $F_0, F_1, F_2, \frac{\partial J}{\partial x}, \frac{\partial J}{\partial y}, \frac{\partial J}{\partial z}$ are linear and

$$\mathrm{Res}_{1,1,1,1,1,1}(F_0, F_1, F_2, \frac{\partial J}{\partial x}, \frac{\partial J}{\partial y}, \frac{\partial J}{\partial z}) = \det(A).$$

Note that each b_{ij} is a cubic polynomial in the c_{ij}'s. Hence the polynomial $\mathrm{Res}(F_0, F_1, F_2, \frac{\partial J}{\partial x}, \frac{\partial J}{\partial y}, \frac{\partial J}{\partial z})$ has total degree 12 in $c_{01}, \ldots, c_{26}$. By Theorem 1, the resultant vanishes iff

$$F_0 = F_1 = F_2 = \frac{\partial J}{\partial x} = \frac{\partial J}{\partial y} = \frac{\partial J}{\partial z} = 0$$

has a nontrivial solution $(x^2, y^2, z^2, xy, xz, yz)$. Also, it can be easily verified that every nontrivial solution of this system is a nontrivial solution of $F_0 = F_1 = F_2 = 0$. Hence (x, y, z) is a nontrivial solution of $F_0 = F_1 = F_2 = 0$. Then $\mathrm{Res}_{2,2,2}(F_0, F_1, F_2) = 0$. Thus $\mathrm{Res}_{2,2,2}(F_0, F_1, F_2)$ vanishes on the set

$$\mathbf{V}(\mathrm{Res}(F_0, F_1, F_2, \frac{\partial J}{\partial x}, \frac{\partial J}{\partial y}, \frac{\partial J}{\partial z})).$$

This means that $\mathrm{Res}_{2,2,2}(F_0, F_1, F_2)$ belongs to the ideal of this variety, i.e.

$$\mathrm{Res}_{2,2,2}(F_0, F_1, F_2) \in \sqrt{\langle \mathrm{Res}(F_0, F_1, F_2, \frac{\partial J}{\partial x}, \frac{\partial J}{\partial y}, \frac{\partial J}{\partial z}) \rangle}.$$

On the other hand, if we substitute every b_{ij} in the above matrix by the corresponding cubic polynomial in the c_{ij}'s, using the function `irreduc` of MAPLE, we can see easily that $\det(A)$ and therefore

$$\mathrm{Res}(F_0, F_1, F_2, \frac{\partial J}{\partial x}, \frac{\partial J}{\partial y}, \frac{\partial J}{\partial z})$$

is irreducible in the c_{ij}'s which yields that

$$\mathrm{Res}_{2,2,2}(F_0, F_1, F_2) \in \langle \mathrm{Res}(F_0, F_1, F_2, \frac{\partial J}{\partial x}, \frac{\partial J}{\partial y}, \frac{\partial J}{\partial z}) \rangle.$$

By Theorem 4, $\mathrm{Res}_{2,2,2}(F_0, F_1, F_2)$ has the total degree 12 in $c_{01}, \ldots, c_{26}$. Hence, for a $c \in K$, we have

$$\mathrm{Res}_{2,2,2}(F_0, F_1, F_2) = c \cdot \mathrm{Res}(F_0, F_1, F_2, \frac{\partial J}{\partial x}, \frac{\partial J}{\partial y}, \frac{\partial J}{\partial z}).$$

But, for the special case; if we set $(F_0, F_1, F_2) = (x^2, y^2, z^2)$, we can conclude that

$$\mathrm{Res}(x^2, y^2, z^2, 8yz, 8xz, 8xy) = \det \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 8 \\ 0 & 0 & 0 & 0 & 8 & 0 \\ 0 & 0 & 0 & 8 & 0 & 0 \end{bmatrix} = -512.$$

Finally, by Theorem 1, we have $\mathrm{Res}_{2,2,2}(x^2, y^2, z^2) = 1$ and so $c = \frac{-1}{512}$. □

ACKNOWLEDGEMENTS

The research of the first author was supported in part by a grant from IPM (No. 93550420). The authors are grateful to the referee and Prof. David Cox for their useful comments and advices for the improvement of this note.

REFERENCES

[1] D. Cox, J. Little, and D. O'Shea, *Using algebraic geometry. 2nd ed.*, 2nd ed. New York, NY: Springer, 2005.
[2] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra. 3rd ed.*, 3rd ed. New York, NY: Springer, 2007.
[3] J. P. Jouanolou, "Le formalisme du résultant. (The formalism of resultant)." *Adv. Math.*, vol. 90, no. 2, pp. 117–263, 1991.
[4] F. Macaulay, "Some formulae in eliminations." *Proc. Lond. Math. Soc.*, vol. 35, pp. 3–27, 1903.
[5] B. Mishra, *Algorithmic algebra.* Berlin: Springer, 1993.
[6] G. Salmon, "Leçons d'algèbre supérieure. Trad. de l'anglais par M. Bazin; augm. de notes par M. Hermite." Paris, Gauthier-Villars. 1868 (1868)., 1868.

Authors' addresses

Amir Hashemi
Department of Mathematical Sciences, Isfahan University of Technology, Isfahan, 84156-83111, Iran School of Mathematics, Institute for Research in Fundamental Sciences (IPM), Tehran, 19395-5746, Iran
E-mail address: Amir.Hashemi@cc.iut.ac.ir

Farzad Mirzavand
Department of Mathematical Sciences, Isfahan University of Technology, Isfahan, 84156-83111, Iran
E-mail address: f.mirzavand@math.iut.ac.ir