# On the History of the Bezoutian and the Resultant Matrix

Harald K. Wimmer
*Mathematisches Institut*
*Universität Würzburg*
*D-8700 Würzburg, West Germany*

Submitted by Thomas Kailath

ABSTRACT

It is shown how the Bezoutian and the resultant matrix evolved from Euler's work in elimination theory.

## 1. INTRODUCTION

Linear systems theory with its emphasis on polynomials and rational functions has created a new demand for those parts of matrix theory which are related to coprimeness and greatest common divisors. The Bezoutian and the resultant matrix are classical tools in that area.

Let $F = \Sigma f_i x^i$ and $G = \Sigma g_j x^j$ be two polynomials over a field $K$ such that $\deg g = m \leqslant \deg f = n$. The Bezoutian

$$B = (b_{ij}) \in K^{n \times n}$$

of $F$ and $G$ is a symmetric matrix defined by

$$\frac{F(x)G(y) - F(y)G(x)}{x - y} = \sum_{i=1}^{n} \sum_{j=1}^{n} x^{i-1} b_{ij} y^{j-1}. \tag{1.1}$$



© Elsevier Science Publishing Co., Inc., 1990
655 Avenue of the Americas, New York, NY 10010 0024-3795/90/$3.50

The resultant matrix is a $(m+n)\times(m+n)$ matrix over $K$ of the form

$$H=\left(F_{(m)},G_{(n)}\right),$$

where

$$F_{(m)}=\underbrace{\begin{pmatrix} f_n & & & \bigcirc \\ \vdots & \ddots & & \\ f_1 & & f_n & \\ f_0 & \ddots & \vdots & f_n \\ & \ddots & f_1 & \vdots \\ & & f_0 & f_1 \\ \bigcirc & & & f_0 \end{pmatrix}}_{m}$$

and

$$G_{(n)}=\underbrace{\begin{pmatrix} g_m & & & \bigcirc \\ \vdots & \ddots & & \\ g_1 & & g_m & \\ g_0 & \ddots & \vdots & g_m \\ & \ddots & g_1 & \vdots \\ & & g_0 & g_1 \\ \bigcirc & & & g_0 \end{pmatrix}}_{n}.$$

It is well known that the matrices $B$ and $H$ provide information on the greatest common divisor of $F$ and $G$.

THEOREM (See e.g. [6]). *For two polynomials $F$ and $G$ the following statements are equivalent*:

(a) $\det B\neq 0$,

(b) $\det H\neq 0$,

(c) $(F,G)=1$.

Both the Bezoutian and the resultant matrix have a history which goes back to the 18th century. In this note I would like to describe the elimination problem which gave rise to the matrices $B$ and $H$. In Euler's *Introduction to Analysis* [4] a system of linear equations appears which has $H$ as its coefficient matrix. Another approach of Euler was elaborated by Bezout [1] and led to the matrix which carries his name.

## 2. ELIMINATION

We start with an example which is taken from Euler's *Introduction* [4, §479]. Let two algebraic curves be given by

$$F(x,y) = f_0 + f_1 y + f_1 y^2 = 0 \tag{2.1}$$

and

$$G(x,y) = g_0 + g_1 y + g_2 y^2 = 0 \tag{2.2}$$

such that $f_i, g_i \in \mathbb{R}[x]$, $i = 0,1,2$, and $f_0 \neq 0$ or $g_0 \neq 0$. In order to find the intersection of the two curves, one might wish to eliminate the indeterminate $y$ from (2.2) and (2.1) to obtain a "resultant equation" $E(x) = 0$. If this is possible, then for each intersection point $(x_0, y_0)$ of the two curves the abscissa $x_0$ is a zero of $E(x) = 0$. In our example,

$$Fg_0 - Gf_0 = y\left[(f_1 g_0 - g_1 f_0) + (f_2 g_0 - g_2 f_0)y\right]$$

implies

$$(f_1 g_0 - g_1 f_0) + (f_2 g_0 - g_2 f_0)y = 0. \tag{2.3}$$

We also have

$$Fg_2 - Gf_2 = (f_0 g_2 - g_0 f_2) + (f_1 g_2 - g_1 f_2)y = 0. \tag{2.4}$$

By eliminating $y$ from (2.3) and (2.4) we obtain the resultant equation

$$E(x) = (f_1 g_0 - g_1 f_0)(f_1 g_2 - g_1 f_2) - (f_2 g_0 - g_2 f_0)^2 = 0. \tag{2.5}$$

Note that the $f_i$'s and $g_k$'s in (2.5) are polynomials in $x$. It is obvious that $E$ is the zero polynomial if $F$ and $G$ have a common factor in $\mathbb{R}[x,y]\backslash\mathbb{R}[x]$.

We now consider the general case of two polynomials in two indeterminates. Let $F,G \in \mathbb{R}[x,y]$ be given by

$$F(x,y) = f_0 + f_1 y + \cdots + f_n y^n$$

and

$$G(x,y) = g_0 + g_1 y + \cdots + g_m y^m \tag{2.6}$$

with $f_i, g_j \in \mathbb{R}[x]$, $i = 0,1,\ldots,n$, $j = 0,1,\ldots,m$, $f_n \neq 0$, and let $(F,G)$ be the ideal generated by $F$ and $G$. If all common divisors of $F$ and $G$ are in $\mathbb{R}[x]$, then the elimination ideal

$$(E) = (F,G) \cap \mathbb{R}[x]$$

is nonzero. In Chapter 19 ("De intersectione curvarum") of [4] Euler presents two methods which lead to a polynomial in $(E)$.

In the first method it is assumed without loss of generality that $m = n$. Euler constructs two polynomials $\tilde{F}, \tilde{G}$ in $(F,G)$ which are of degree less than $n$ in $y$. Define

$$\tilde{F} = F g_n - G f_n$$

and

$$\begin{aligned}\tilde{G} = {} & F\left(g_n y^{n-1} + g_{n-1} y^{n-2} + \cdots + g_1\right) \\ & - G\left(f_n y^{n-1} + f_{n-2} y^{n-2} + \cdots + f_1\right).\end{aligned}$$

Then

$$\tilde{F} = \sum_{i=0}^{n-1} (f_i g_n - g_i f_n) y^i.$$

Step by step the degree is pushed down until the algorithm terminates with a polynomial in $\mathbb{R}[x]$.

In his second method Euler obtains a polynomial in $(E)$ by solving a system of linear equations. The goal—in Euler's words [4]—is to fuse the equations $F(x, y) = 0$ and $G(x, y) = 0$ into a single equation which does not contain $y$ any more. For that purpose multiply $F$ by

$$A(x,y) = \sum_{\mu=0}^{m-1} a_\mu y^\mu, \qquad a_\mu \in \mathbb{R}(x)$$

and $G$ by

$$B(x,y) = \sum_{\nu=0}^{n-1} b_\nu y^\nu, \qquad b_\nu \in \mathbb{R}(x).$$

The coefficients $a_\mu$, $b_\nu$ are to be determined in such a way that the terms in $FA$ and $GB$ which belong to the same powers of $y$ are "mutually destroyed." Then $FA = GB$ is the desired equation from which $y$ is absent. Euler puts $a_{m-1} = g_m$ and $b_{n-1} = f_n$ and notes the following equations:

$$f_n g_m = f_n g_m,$$

$$f_n a_{m-2} + f_{n-1} g_m = g_m b_{n-1} + g_{m-1} f_n,$$

$$f_n a_{m-3} + f_{n-1} a_{m-2} + f_{n-2} g_m = g_m b_{n-2} + g_{m-1} b_{n-1} + g_{m-2} f_n,$$

$$f_n a_{m-4} + f_{n-1} a_{m-3} + f_{n-2} a_{m-2} + f_{n-3} g_m = g_m b_{n-3} + g_{m-1} b_{n-2} + g_{m-2} b_{n-1} + g_{m-1} f_n.$$

$$\vdots$$

If we define $c = f_0 a_0 - g_0 b_0$ then $c \in \mathbb{R}(x)$. Euler's approach is described by the linear system

$$(F_{(m)}, -G_{(n)})(a_{m-1}, \dots, a_0, b_{n-1}, \dots, b_0)^T = (0, \dots, 0, c)^T, \qquad (2.7)$$

$$a_{m-1} = g_m, \qquad b_{n-1} = f_n.$$

Except for the minus sign of $G_{(n)}$, the coefficient matrix of (2.7) is the resultant matrix $H$ of $F$ and $G$, and $\det H \in (E)$.

In his memoir [1] Bezout goes beyond Euler's degree reduction method. Again let $m = n$ in (2.6). From $F$ and $G$, $n$ equations of degree $n-1$ are derived which allow a simultaneous elimination of $y$. Put

$$F^{(i)} = f_i + f_{i+1}y + \cdots + f_n y^{n-i}$$

and

$$G^{(i)} = g_i + g_{i+1}y + \cdots + g_n y^{n-1},$$

$i = 1, 2, \dots, n$, and define

$$B^{(i)} = FG^{(i)} - GF^{(i)}, \qquad i = 1, 2, \dots, n.$$

Then $B^{(i)} = (f_0 + \cdots + f_{i-1}y^{(i-1)})G^{(i)} - (g_0 + \cdots + g_{i-1}y^{i-1})F^{(i)}$ is of degree $n-1$ in $y$ and $B^{(i)} \in (F, G)$. Note that Euler worked with the first and the last of those polynomials, namely with $B^{(1)}$ and $B^{(n)}$. Now let a matrix $B \in \mathbb{R}^{n\times n}[x]$ be defined by

$$\begin{pmatrix} B^{(1)} \\ \vdots \\ B^{(n)} \end{pmatrix} = B \begin{pmatrix} 1 \\ y \\ \vdots \\ y^{n-1} \end{pmatrix}. \tag{2.8}$$

Bezout [1, p. 319] considers the powers $y^\nu$, $\nu = 0, \dots, n-1$, as unknowns in a system of $n$ linear equations given by (2.8). Based on Cramer's results on determinants, one has to determine the necessary condition for the solvability of the $n$ linear equations, which yields an (algebraic) equation in $x$. Bezout actually works out completely an example of degree $n = 4$. He suggests that one might establish a general rule for equations of arbitrary high degree. "But," he adds, "this is a task to which I invite those who are lucky enough to have more time at their disposal than I do" [1, pp. 328–329].

With the determinant and the adjoint of $B$ we can argue as follows. Let $(c_1, \dots, c_n) \in \mathbb{R}^{1\times n}[x]$ be the first row of adj$(B)$. Then (2.8) implies

$$\operatorname{adj}(B)\begin{pmatrix} B^{(1)} \\ \vdots \\ B^{(n)} \end{pmatrix} = \det B \begin{pmatrix} 1 \\ y \\ \vdots \\ y^{n-1} \end{pmatrix},$$

and

$$\sum_{i=1}^{n} c_i B^{(i)} = \det B.$$

Therefore

$$\det B \in (F, G) \cap \mathbb{R}[x].$$

We observe that the generating polynomial (1.1) does not appear in Bezout's paper [1]. From

$$B\begin{pmatrix} 1 \\ y \\ \vdots \\ y^{n-1} \end{pmatrix} = \begin{pmatrix} B^{(1)} \\ \vdots \\ B^{(n)} \end{pmatrix} = F\begin{pmatrix} G^{(1)} \\ \vdots \\ G^{(n)} \end{pmatrix} - G\begin{pmatrix} F^{(1)} \\ \vdots \\ F^{(n)} \end{pmatrix} \tag{2.9}$$

the following representation of $B$ is immediate:

$$B = \begin{pmatrix} f_1 & f_2 & \cdot & \cdot & \cdot & f_n \\ f_2 & & & & \cdot & \\ \vdots & & & \cdot & & \\ \cdot & & \cdot & & & \\ f_n & & & & & \bigcirc \end{pmatrix}\begin{pmatrix} g_0 & \cdot & \cdot & \cdot & g_{n-2} & g_{n-1} \\ & \cdot & & & & g_{n-2} \\ & & \cdot & & & \vdots \\ & & & \cdot & & \cdot \\ \bigcirc & & & & & g_0 \end{pmatrix}$$

$$- \begin{pmatrix} g_1 & g_2 & \cdot & \cdot & \cdot & g_n \\ g_2 & & & & \cdot & \\ \vdots & & & \cdot & & \\ \cdot & & \cdot & & & \\ g_n & & & & & \bigcirc \end{pmatrix}\begin{pmatrix} f_0 & \cdot & \cdot & \cdot & f_{n-2} & f_{n-1} \\ & \cdot & & & & f_{n-2} \\ & & \cdot & & & \vdots \\ & & & \cdot & & \cdot \\ \bigcirc & & & & & f_0 \end{pmatrix}. \tag{2.10}$$

Hence (2.10) should be considered as Bezout's matrix.

It was Cayley [2] who claimed that the matrices $B$ in (1.1) and (2.9) are the same. He proved his statement for $n = 2$ and $n = 3$. (This is another illustration of Cayley's attitude that proofs were only a secondary aspect of mathematical discovery [3].)

A more detailed investigation of Bezout's system of equations (2.8) and the corresponding coefficient matrix $B$ was made by Jacobi. In [5] Jacobi points out that $B$ is symmetric and that

$$\sum_{i,j=1}^{n-1} x^{i-1} b_{ij} x^{j-1} = F(x)G'(x) - G(x)F'(x).$$

He also shows that $\det B = 0$ implies the existence of a common factor $D$ of $F$ and $G$.

In the work of all the authors mentioned above, the coefficients of $F$ and $G$ are polynomials. If the preceding methods are used for elimination in $\mathbb{R}[x]$, then the matrices $H$ and $B$ which are associated to $F, G \in \mathbb{R}[x]$ have their entries in $\mathbb{R}$. The elimination ideal $(F,G) \cap \mathbb{R}$ is either (1) or (0). Hence $\det H \neq 0$ (or equivalently $\det B \neq 0$) if and only if $(F,G) = 1$.

## REFERENCES

1 É. Bezout, Recherches sur le degré des équations résultantes de l'évanouissement des inconnues, et sur les moyens qu'il convient d'employer pour trouver ces équations, *Mém. Acad. Roy. Sci. Paris*, 1764, pp. 288–338.
2 A. Cayley, Note sur la méthode d'élimination de Bezout, *J. Reine Angew. Math.* 53:366–367 (1857).
3 J. Dieudonné, *Abrégé d'Histoire des Mathématiques 1700–1900*, Tome I, Hermann, Paris, 1978.
4 L. Euler, *Introductio in Analysin Infinitorum*, Tom. 2, Lausanne, 1748.
5 C. G. J. Jacobi, De eliminatione variabilis e duabus aequationibus algebraicis, *J. Reine Angew. Math.* 15:101–124 (1836).
6 T. Kailath, *Linear Systems*, Prentice-Hall, Englewood Cliffs, N.J., 1980.

*Received 18 July 1988; final manuscript accepted 16 November 1988*