PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 54, January 1976

THE RESULTANT OF SEVERAL HOMOGENEOUS POLYNOMIALS IN TWO INDETERMINATES

KUNIO KAKIÉ

ABSTRACT. We give one method of determining the degree of the highest common factor of several homogeneous polynomials in two indeterminates.

0. **Introduction.** Let us consider r homogeneous polynomials in two indeterminates. The problem to engage our attention is to determine the degree of their highest common factor. When $r = 2$, the classical elimination theory gives a condition in order that two polynomials have a common nonconstant factor (cf. B. L. van der Waerden [3, vol. I, Chapter 4]; R. J. Walker [4, Chapter I]). In the general case when $r \geq 2$, B. L. van der Waerden gave one condition in order that r polynomials have a common nonconstant factor [3, vol. II, Chapter 11]. It is not difficult to complete this theory in order to give an answer to the problem proposed above (see Propositions 1, 2; cf. J. M. Thomas [2, Chapter V]). In this paper, we give another answer to the above problem in the general case (Theorems A and A*). This result seems to be a more natural generalization of the classical resultant theory in the case of two polynomials. Moreover it leads to a theorem (Theorem in §5) which possesses a fruitful application to the theory of involutive systems of partial differential equations in two independent variables (cf. K. Kakié [1]).

The author wishes to express his sincere gratitude to Professor R. J. Walker for correcting some errors.

1. **Main results.** Let K be a field and let $K[x,y]$ denote the ring of polynomials in two indeterminates x, y. Let us consider r homogeneous polynomials belonging to $K[x,y]$ of degrees $n_1, n_2, \ldots, n_r$ respectively:

$$P_\alpha(x,y) = A_0^{(\alpha)} x^{n_\alpha} + A_1^{(\alpha)} x^{n_\alpha - 1} y + \cdots + A_{n_\alpha}^{(\alpha)} y^{n_\alpha} \qquad (\alpha = 1, 2, \ldots, r).$$

We shall write

$$n^* = \max\{n_\alpha; 1 \leq \alpha \leq r\}, \qquad n_* = \min\{n_\alpha; 1 \leq \alpha \leq r\}.$$

Recalling the classical theory of resultants, we introduce the following matrix for each integer $l \geq n^*$:

Received by the editors November 9, 1974.
AMS (MOS) subject classifications (1970). Primary 10M05.
Key words and phrases. Polynomials, (highest) common factor, resultant.

$$R_l = \begin{bmatrix} A_0^{(1)} & A_1^{(1)} \cdot & \cdots & \cdot A_{n_1}^{(1)} & & & \\ & A_0^{(1)} & A_1^{(1)} \cdot & \cdots & \cdot A_{n_1}^{(1)} & & \\ & & \cdots & \cdots & \cdots & & \\ & & & A_0^{(1)} & A_1^{(1)} \cdot & \cdots & \cdot A_{n_1}^{(1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ A_0^{(r)} & A_1^{(r)} \cdot & \cdots & \cdot A_{n_r}^{(r)} & & & \\ & A_0^{(r)} & A_1^{(r)} \cdot & \cdots & \cdot A_{n_r}^{(r)} & & \\ & & \cdots & \cdots & \cdots & & \\ & & & A_0^{(r)} & A_1^{(r)} \cdot & \cdots & \cdot A_{n_r}^{(r)} \end{bmatrix},$$

there being $l - n_\alpha + 1$ rows of $A^{(\alpha)}$'s for each $\alpha = 1, 2, \ldots, r$ and $l + 1$ columns, the blank spaces being filled with zeros.

We shall now state our results.

THEOREM A. *In order that the polynomials $P_1, P_2, \ldots, P_r$ have a common factor of degree $\geq k$, it is necessary and sufficient that* rank $R_{n^*+n_*-k}$ *is less than* $n^* + n_* - 2k + 2$.

This result is completed by

THEOREM A*. *The highest common factor of the polynomials $P_1, P_2, \ldots, P_r$ is of degree k if and only if*

$$\begin{cases} \text{rank } R_{n^*+n_*-k-1} = n^* + n_* - 2k, \\ \text{rank } R_{n^*+n_*-k} = \text{rank } R_{n^*+n_*-k-1} + 1. \end{cases}$$

2. **The case of two polynomials.** Let $P(x,y)$ and $Q(x,y)$ be homogeneous polynomials belonging to $K[x,y]$ of degrees n and m respectively:

$$P(x,y) = A_0 x^n + A_1 x^{n-1} y + \cdots + A_n y^n,$$

$$Q(x,y) = B_0 x^m + B_1 x^{m-1} y + \cdots + B_m y^m.$$

It is remarked that any factor of a homogeneous polynomial is necessarily homogeneous (cf. R. J. Walker [4, Chapter I, §10]).

PROPOSITION 1. *P and Q have a common factor of degree $\geq k$ if and only if the rank of the following matrix is less than $n + m - 2k + 2$:*

$$\begin{bmatrix} A_0 & A_1 \cdot & \cdots & \cdot A_n & & \\ & A_0 & A_1 \cdot & \cdots & \cdot A_n & \\ & & \cdots & \cdots & \cdots & \\ & & & A_0 & A_1 \cdot & \cdot A_n \\ B_0 & B_1 \cdot & \cdots & \cdot B_m & & \\ & B_0 & B_1 \cdot & \cdots & \cdot B_m & \\ & & \cdots & \cdots & \cdots & \\ & & & B_0 & B_1 \cdot & \cdot B_m \end{bmatrix},$$

there being $m-k+1$ rows of A 's, $n-k+1$ rows of B 's and $n+m-k+1$ columns in the matrix, the blank spaces being filled with zeros.

PROOF. This is proved in just the same manner as in the argument stated in B. L. van der Waerden [3, Chapter 4, §27] or R. J. Walker [4, Chapter I, §9]. In fact, it is easy to see that P and Q have a common factor of degree $\geq k$ if and only if there exist two homogeneous polynomials H and G belonging to $K[x,y]$ of degrees $m-k$ and $n-k$ respectively such that $HP = GQ$. As is readily seen, such polynomials exist if and only if the condition in the proposition is satisfied. Q.E.D.

3. **The case of more than two polynomials of the same degree.** We consider r homogeneous polynomials of $K[x,y]$ having the same degree n

$$Q_\alpha(x,y) = B_0^{(\alpha)}x^n + B_1^{(\alpha)}x^{n-1}y + \cdots + B_n^{(\alpha)}y^n \qquad (\alpha = 1,2,\ldots,r).$$

In order that a polynomial is a common factor of $Q_1, \ldots, Q_r$, it is necessary and sufficient that it is a common factor of $\sum_{\alpha=1}^r Q_\alpha u_\alpha$ and $\sum_{\alpha=1}^r Q_\alpha v_\alpha$, where u's and v's represent $2r$ indeterminates. Applying Proposition 1, we can immediately obtain the following result (cf. van der Waerden [3, Chapter 11, §77]).

PROPOSITION 2. *The polynomials $Q_1, Q_2, \ldots, Q_r$ have a common factor of degree $\geq k$ if and only if the rank of the following matrix is less than $2(n-k+1)$:*

$$\begin{bmatrix}
\Sigma B_0^{(\alpha)}u_\alpha & \Sigma B_1^{(\alpha)}u_\alpha & \cdots & \Sigma B_n^{(\alpha)}u_\alpha & & \\
 & \Sigma B_0^{(\alpha)}u_\alpha & \Sigma B_1^{(\alpha)}u_\alpha & \cdots & \Sigma B_n^{(\alpha)}u_\alpha & \\
 & & \cdots & \cdots & \cdots & \\
 & & \Sigma B_0^{(\alpha)}u_\alpha & \Sigma B_1^{(\alpha)}u_\alpha & \cdots & \Sigma B_n^{(\alpha)}u_\alpha \\
\Sigma B_0^{(\alpha)}v_\alpha & \Sigma B_1^{(\alpha)}v_\alpha & \cdots & \Sigma B_n^{(\alpha)}v_\alpha & & \\
 & \Sigma B_0^{(\alpha)}v_\alpha & \Sigma B_1^{(\alpha)}v_\alpha & \cdots & \Sigma B_n^{(\alpha)}v_\alpha & \\
 & & \cdots & \cdots & \cdots & \\
 & & \Sigma B_0^{(\alpha)}v_\alpha & \Sigma B_1^{(\alpha)}v_\alpha & \cdots & \Sigma B_n^{(\alpha)}v_\alpha
\end{bmatrix},$$

there being $n-k+1$ rows of $\sum B_i^{(\alpha)}u_\alpha$, $n-k+1$ rows of $\sum B_i^{(\alpha)}v_\alpha$, the blank spaces being filled with zeros.

Let us now state our condition in order that $Q_1, \ldots, Q_r$ have a common factor of degree $\geq k$. We shall denote by S_l the matrix R_l constructed from $Q_1, \ldots, Q_r$:

$$S_l = \begin{bmatrix} B_0^{(1)} & B_1^{(1)} & \cdots & \cdots & B_n^{(1)} & & & \\ & B_0^{(1)} & B_1^{(1)} & \cdots & \cdots & B_n^{(1)} & & \\ & & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & & B_0^{(1)} & B_1^{(1)} & \cdots & \cdots & B_n^{(1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ B_0^{(r)} & B_1^{(r)} & \cdots & \cdots & B_n^{(r)} & & & \\ & B_0^{(r)} & B_1^{(r)} & \cdots & \cdots & B_n^{(r)} & & \\ & & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & & B_0^{(r)} & B_1^{(r)} & \cdots & \cdots & B_n^{(r)} \end{bmatrix},$$

there being $l - n + 1$ rows of $B^{(\alpha)}$'s for each $\alpha = 1, 2, \ldots, r$, the blank spaces being filled with zeros.

PROPOSITION 3. *The r polynomials $Q_1, Q_2, \ldots, Q_r$ have a common factor of degree $\geq k$ if and only if the matrix S_{2n-k} has rank less than* $2(n - k + 1)$.

Before proving this proposition, we prepare a lemma concerning the ranks of R's (and hence S's).

LEMMA. *Assume that* rank $R_{n^*+n_*-k}$ *is less than* $n^* + n_* - 2k + 2$. *Then for each integer* $a \geq 0$

$$\operatorname{rank} R_{n^*+n_*-k+a} = \operatorname{rank} R_{n^*+n_*-k} + a.$$

PROOF. We shall prove that for each integer $l \geq n^* + n_* - k$, rank R_{l+1} = rank $R_l + 1$. For brevity we denote rank R_l by γ_l. We say that the νth row of R_l is independent or dependent according as it is linearly independent or linearly dependent of the first $\nu - 1$ row-vectors of R_l, and we call the $l - n_\alpha + 1$ rows of R_l constructed from the coefficients of P_α the αth block of R_l. We first prove $\gamma_{n^*+n_*-k+1} = \gamma_{n^*+n_*-k} + 1$. Without loss of generality we may assume that $n_1 = n_*$. From the assumption that $\gamma_{n^*+n_*-k} < (n^* - k + 1) + (n_* - k + 1)$, we easily see that there exists at least one dependent row in each block of $R_{n^*+n_*-k}$ except the first, and that for any $\alpha = 2, 3, \ldots, r$ the νth row of $R_{n^*+n_*-k}$ belonging to the αth block is dependent, $(\alpha + \nu - 1)$th row and $(\alpha + \nu)$th row of $R_{n^*+n_*-k+1}$ are dependent. This fact shows that the number of independent rows of $R_{n^*+n_*-k+1}$ is greater than the number of independent rows of $R_{n^*+n_*-k}$ at most by one; that is, $\gamma_{n^*+n_*-k+1} \leq \gamma_{n^*+n_*-k} + 1$. On the other hand, noticing the form of matrices R's, we have that rank $R_{l+1} - 1 \geq$ rank R_l for any integer $l \geq n^*$. In particular, $\gamma_{n^*+n_*-k+1} \geq \gamma_{n^*+n_*-k} + 1$. Hence we have $\gamma_{n^*+n_*-k+1} = \gamma_{n^*+n_*-k} + 1$. In the same manner we can prove that $\gamma_{l+1} = \gamma_l + 1$ for each integer $l \geq n^* + n_* - k$. What we have proved shows that $\gamma_{n^*+n_*-k+a} = \gamma_{n^*+n_*-k} + a$. Q.E.D.

PROOF OF PROPOSITION 3. *Sufficiency*. By multiplying the αth block composed of the $n - k + 1$ rows of S_{2n-k} constructed from the coefficients of Q_α by u_α (resp. v_α) and adding them, we can construct the matrix in Proposition 2 and we readily see that the condition stated in Proposition 2 is satisfied.

Hence $Q_1, \ldots, Q_r$ have a common factor of degree $\geq k$.

Necessity. We say that a vector $\mathbf{c} = (c_1, c_2, \ldots, c_a)$ is a null-vector of a matrix M with a rows and b columns if $\mathbf{c}M = 0$. To a vector

$$\mathbf{e} = (e_0^{(1)}, e_1^{(1)}, \ldots, e_{n-k}^{(1)}, e_0^{(2)}, e_1^{(2)}, \ldots, e_{n-k}^{(2)}, \ldots, e_0^{(r)}, e_1^{(r)}, \ldots, e_{n-k}^{(r)})$$

we can correspond the set of ordered r homogeneous polynomials, $(H_1, H_2, \ldots, H_r)$, of degree $n-k$ where

$$H_\alpha(x,y) = e_0^{(\alpha)} x^{n-k} + e_1^{(\alpha)} x^{n-k-1} y + \cdots + e_{n-k}^{(\alpha)} y^{n-k} \qquad (\alpha = 1, 2, \ldots, r).$$

We say that the vector $\mathbf{e}$ and the set of ordered r polynomials $(H_1, H_2, \ldots, H_r)$ are associated with each other. The finite sets of ordered r homogeneous polynomials are said to be independent of one another if the vectors associated with them are linearly independent over K. By the same argument as in the proof of Proposition 1 (cf. van der Waerden [3, Chapter 4, §27]), we see that the vector $\mathbf{e}$ is a null-vector of the matrix S_{2n-k} if and only if the set of ordered r polynomials $(H_1, \ldots, H_r)$ associated with it satisfies the relation

$$(1) \qquad H_1(x,y)Q_1(x,y) + H_2(x,y)Q_2(x,y) + \cdots + H_r(x,y)Q_r(x,y) = 0.$$

Assume that Q_α $(1 \leq \alpha \leq r)$ have a common factor of degree $\geq k$. We shall first prove the assertion in the case when they have a common factor $C(x,y)$ exactly of degree k. We can write $Q_\alpha = q_\alpha C$, where q_α are homogeneous polynomials of degree $n-k$;

$$q_\alpha(x,y) = a_0^{(\alpha)} x^{n-k} + a_1^{(\alpha)} x^{n-k-1} y + \cdots + a_{n-k}^{(\alpha)} y^{n-k} \qquad (\alpha = 1, 2, \ldots, r).$$

From the above fact we see that S_{2n-k} has rank less than $2(n-k+1)$ if and only if there exist at least $(r-2)(n-k+1)+1$ independent sets of ordered r homogeneous polynomials of degree $n-k$ which satisfy relation (1). On the other hand, a set of r polynomials $(H_1, \ldots, H_r)$ satisfies (1) if and only if it satisfies

$$(2) \qquad H_1(x,y)q_1(x,y) + H_2(x,y)q_2(x,y) + \cdots + H_r(x,y)q_r(x,y) = 0.$$

Let us construct a matrix with $r(n-k+1)$ rows and $2(n-k+1)-1$ columns:

$$\begin{bmatrix}
a_0^{(1)} & a_1^{(1)} & \cdots & a_{n-k}^{(1)} & & & \\
& a_0^{(1)} & a_1^{(1)} & \cdots & a_{n-k}^{(1)} & & \\
& & \cdots & \cdots & \cdots & \cdots & \\
& & & a_0^{(1)} & a_1^{(1)} & \cdots & a_{n-k}^{(1)} \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
a_0^{(r)} & a_1^{(r)} & \cdots & a_{n-k}^{(r)} & & & \\
& a_0^{(r)} & a_1^{(r)} & \cdots & a_{n-k}^{(r)} & & \\
& & \cdots & \cdots & \cdots & \cdots & \\
& & & a_0^{(r)} & a_1^{(r)} & \cdots & a_{n-k}^{(r)}
\end{bmatrix},$$

there being $n - k + 1$ rows of $a^{(\alpha)}$'s for each $\alpha = 1, 2, \ldots, r$, the blank spaces being filled with zeros. Clearly there exist at least $(r-2)(n-k+1)+1$ independent null-vectors of the above matrix. Hence, by the same reasoning as before, there exist at least $(r-2)(n-k+1)+1$ independent sets of ordered r homogeneous polynomials of degree $n-k$ which satisfy relation (2). By the fact already remarked, this shows that S_{2n-k} has rank less than $2(n-k+1)$. Let us now prove the assertion in the general case when Q's have a common factor of degree $\geq k$. Suppose that they have a common factor of degree $h \geq k$. Then by the result already proved, rank S_{2n-h} is less than $2(n-h+1)$. By the above Lemma, rank $S_{2n-k} =$ rank $S_{2n-h} + (h-k)$. Therefore rank S_{2n-k} is less than $2(n-h+1)+(h-k) \leq 2(n-k+1)$. Thus the proof of necessity is complete. Q.E.D.

4. **Proofs of Theorems A and A*.** The proof of Theorem A: A polynomial is a common factor of the polynomials $P_1, \ldots, P_r$ if and only if it is a common factor of the polynomials

$$(3) \qquad \begin{cases} P_1(x,y)x^{n^*-n_1-i}y^i & (0 \leq i \leq n^*-n_1), \\ P_2(x,y)x^{n^*-n_2-i}y^i & (0 \leq i \leq n^*-n_2), \\ \cdots\cdots\cdots\cdots\cdots\cdots & \\ P_r(x,y)x^{n^*-n_r-i}y^i & (0 \leq i \leq n^*-n_r). \end{cases}$$

Apply Proposition 3 to the polynomials (3) of degree n^* and transform adequately the matrix in the obtained condition, then we see that the polynomials (3) have a common factor of degree $\geq k$ if and only if rank R_{2n^*-k} is less than $2(n^*-k+1)$. In order to complete the proof, it is necessary to show that rank R_{2n^*-k} is less than $2(n^*-k+1)$ if and only if rank $R_{n^*+n_*-k}$ is less than n^*+n_*-2k+2. As remarked in the proof of the Lemma in §3, rank $R_{l+1} - 1 \geq$ rank R_l for each integer $l \geq n^*$. Hence if rank R_{2n^*-k} is less than $2(n^*-k+1)$, then rank R_{2n^*-k-1} is less than $2(n^*-k+1)-1$. If we use the above inequality (n^*-n_*)-times successively, then we find that rank $R_{n^*+n_*-k}$ is less than n^*+n_*-2k+2. Conversely assume that rank $R_{n^*+n_*-k}$ is less than n^*+n_*-2k+2. By the Lemma, rank R_{2n^*-k} is equal to rank $R_{n^*+n_*-k}+(n^*-n_*)$. Hence rank R_{2n^*-k} is less than $2(n^*-k+1)$. Q.E.D.

THE PROOF OF THEOREM A*. If rank $R_{n^*+n_*-k-1}$ is less than n^*+n_*-2k, then by Theorem A the degree of the highest common factor of $P_1, \ldots, P_r$ is greater than k. If rank $R_{n^*+n_*-k-1}$ is greater than n^*+n_*-2k, then it follows that rank $R_{n^*+n_*-k}$ is equal to or greater than n^*+n_*-2k+2. Therefore, by Theorem A, the highest common factor of $P_1, \ldots, P_r$ has degree less than k. Hence the assertion is an immediate consequence of Theorem A. Q.E.D.

5. **Supplementary result.** We shall deduce from Theorem A* a theorem which possesses an application to the theory of partial differential equations in two independent variables (cf. K. Kakié [1]). Consider the polynomials $Q_1, Q_2, \ldots, Q_r$ of the same degree n given in §3.

THEOREM. *Suppose that* rank S_{n+1} = rank $S_n + 1$. *Then the degree of the highest common factor of* $Q_1, \ldots, Q_r$ *is equal to* $n + 1 -$ rank S_n.

PROOF. The assumption implies that rank S_l = rank $S_n + l - n$. Hence we readily obtain the following equality:

$$\operatorname{rank} S_{2n-(n+1-\delta)-1} = 2\delta - 2 = 2\{n - (n + 1 - \delta)\},$$

where δ = rank S_n. Hence by Theorem A*, we obtain the desired result. Q.E.D.

An elementary proof of this theorem given by M. Matsuda is found in K. Kakié [1, §3, Lemma 2].

REFERENCES

1. K. Kakié, *On involutive systems of partial differential equations in two independent variables*, J. Fac. Sci. Univ. Tokyo sect. IA **21** (1974), 405–433.

2. J. M. Thomas, *Differential systems*, Amer. Math. Soc. Colloq. Publ., vol. 21, Amer. Math. Soc., Providence, R. I., 1937.

3. B. L. van der Waerden, *Moderne Algebra*. Vols. I, II, Zweite Auflage, Springer, Berlin, 1937, 1940; English transl., Ungar, New York, 1949, 1950. MR **10**, 587.

4. R. J. Walker, *Algebraic curves*, Princeton Math. Ser., vol. 13, Princeton Univ. Press, Princeton, N. J., 1950. MR **11**, 387.

DEPARTMENT OF MATHEMATICS, RIKKYO UNIVERSITY, NISHI-IKEBUKURO, TOKYO 171, JAPAN