

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  $n_1, n_2, \dots, n_r$  respectively:

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

We shall write

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

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.

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

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

We shall now state our results.

**THEOREM A.** *In order that the polynomials  $P_1, P_2, \dots, P_r$  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  $P_1, P_2, \dots, P_r$  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:

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

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

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  $n + m - 2k + 2$ :*

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

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  $n$

$$Q_\alpha(x, y) = B_0^{(\alpha)}x^n + B_1^{(\alpha)}x^{n-1}y + \dots + B_n^{(\alpha)}y^n$$

$$(\alpha = 1, 2, \dots, r).$$

In order that a polynomial is a common factor of  $Q_1, \dots, Q_r$ , 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  $Q_1, Q_2, \dots, Q_r$  have a common factor of degree  $\geq k$  if and only if the rank of the following matrix is less than  $2(n - k + 1)$ :*

$$\left[ \begin{array}{cccccccc} \sum B_0^{(\alpha)} u_\alpha & \sum B_1^{(\alpha)} u_\alpha & \cdot & \cdot & \cdot & \cdot & \cdot & \sum B_n^{(\alpha)} u_\alpha \\ & \sum B_0^{(\alpha)} u_\alpha & \sum B_1^{(\alpha)} u_\alpha & \cdot & \cdot & \cdot & \cdot & \sum B_n^{(\alpha)} u_\alpha \\ & & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & & \sum B_0^{(\alpha)} u_\alpha & \sum B_1^{(\alpha)} u_\alpha & \cdot & \cdot & \cdot & \sum B_n^{(\alpha)} u_\alpha \\ \sum B_0^{(\alpha)} v_\alpha & \sum B_1^{(\alpha)} v_\alpha & \cdot & \cdot & \cdot & \cdot & \cdot & \sum B_n^{(\alpha)} v_\alpha \\ & \sum B_0^{(\alpha)} v_\alpha & \sum B_1^{(\alpha)} v_\alpha & \cdot & \cdot & \cdot & \cdot & \sum B_n^{(\alpha)} v_\alpha \\ & & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & & \sum B_0^{(\alpha)} v_\alpha & \sum B_1^{(\alpha)} v_\alpha & \cdot & \cdot & \cdot & \sum B_n^{(\alpha)} v_\alpha \end{array} \right],$$

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  $Q_1, \dots, Q_r$  have a common factor of degree  $\geq k$ . We shall denote by  $S_l$  the matrix  $R_l$  constructed from  $Q_1, \dots, Q_r$ :

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

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

**PROPOSITION 3.** *The  $r$  polynomials  $Q_1, Q_2, \dots, Q_r$  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  $\text{rank } R_{n^*+n_*-k}$  is less than  $n^* + n_* - 2k + 2$ . Then for each integer  $a \geq 0$*

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

**PROOF.** We shall prove that for each integer  $l \geq n^* + n_* - k$ ,  $\text{rank } R_{l+1} = \text{rank } R_l + 1$ . For brevity we denote  $\text{rank } R_l$  by  $\gamma_l$ . We say that the  $\nu$ th 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  $P_\alpha$  the  $\alpha$ th 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  $\alpha = 2, 3, \dots, r$  the  $\nu$ th row of  $R_{n^*+n_*-k}$  belonging to the  $\alpha$ th 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  $\text{rank } R_{l+1} - 1 \geq \text{rank } R_l$  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  $\alpha$ th block composed of the  $n - k + 1$  rows of  $S_{2n-k}$  constructed from the coefficients of  $Q_\alpha$  by  $u_\alpha$  (resp.  $v_\alpha$ ) and adding them, we can construct the matrix in Proposition 2 and we readily see that the condition stated in Proposition 2 is satisfied.





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

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

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

where  $\delta = \text{rank } S_n$ . 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