THE MINIMAL NUMBERS OF BINARY FORMS[1]

RUFUS OLDENBURGER AND ARTHUR PORGES

1. **Introduction.** One of us proved that for certain fields K a form F of degree m can be written as a linear combination of mth powers of linear forms. Such a combination is termed a *representation* of F and the least possible number of terms in any such representation is called the *minimal* number of F with respect to K. The minimal number depends on both F and K. For fields K with characteristic greater than n, and binary forms F of degree n, it has been proved[2] that the minimal number ranges over at least $1, 2, \cdots, n$, and at most $1, 2, \cdots, n+1$, but the exact range was not determined. In the present paper the authors prove that the range is precisely $1, 2, \cdots, n$.

2. **Preliminary lemmas.** In what follows we use *identity* of polynomials in the usual sense, namely polynomials P and Q are identical if the coefficients of P equal the corresponding coefficients of Q.

Since the order of a field K is greater than m if the characteristic of K is greater than m, we have the following lemma.

LEMMA 1. *For a field K with characteristic greater than m a polynomial P of degree m is equal to a polynomial Q for all values of the variables if and only if P and Q are identical.*

An immediate consequence of Lemma 1 is the following lemma.

LEMMA 2. *For a field K with characteristic greater than m, a polynomial P of degree m not identically zero is different from zero for at least one set of values of the variables.*

LEMMA 3. *Let K be a field with characteristic greater than m. Let Δ be the determinant*

$$(1)\qquad \Delta = \begin{vmatrix} 1 & \cdots & 1 & b_1 \\ a_1 & \cdots & a_m & b_2 \\ \cdot & \cdots & \cdot & \cdot \\ a_1^m & \cdots & a_m^m & b_{m+1} \end{vmatrix}$$

of order $m+1$, $m \geqq 1$, with elements in K, and suppose that the b's are not all zero. The determinant Δ is not identically zero in the a's.

[1] Presented to the Society, April 13, 1940.

[2] R. Oldenburger, *Polynomials in several variables*, Annals of Mathematics, (2), vol. 41 (1940), no. 3, pp. 694–710.

Lemma 3 is valid when $m=1$. For $m \geqq 2$ we have the following sequence of equalities:

$$\Delta = \begin{vmatrix} 1 & 0 & \cdots & 0 & b_1 \\ a_1 & (a_2 - a_1) & \cdots & (a_m - a_1) & b_2 \\ a_1^2 & (a_2^2 - a_1^2) & \cdots & (a_m^2 - a_1^2) & b_3 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ a_1^m & (a_2^m - a_1^m) & \cdots & (a_m^m - a_1^m) & b_{m+1} \end{vmatrix}$$

$$= (a_2 - a_1) \cdots (a_m - a_1) \begin{vmatrix} 1 & 0 & \cdots 0 & b_1 \\ 0 & 1 & \cdots 1 & (b_2 - b_1 a_1) \\ 0 & a_2 & \cdots a_m & (b_3 - b_2 a_1) \\ \cdot & \cdot & \cdots \cdot & \cdot \\ 0 & a_2^{m-1} & \cdots a_m^{m-1} & (b_{m+1} - b_m a_1) \end{vmatrix}.$$

Thus

$$\Delta = (a_2 - a_1) \cdots (a_m - a_1)(M - a_1 N), \tag{2}$$

where

$$M = \begin{vmatrix} 1 & \cdots 1 & b_2 \\ a_2 & \cdots a_m & b_3 \\ a_2^2 & \cdots a_m^2 & b_4 \\ \cdot & \cdots \cdot & \cdot \\ a_2^{m-1} & \cdots a_m^{m-1} & b_{m+1} \end{vmatrix}, \qquad N = \begin{vmatrix} 1 & \cdots 1 & b_1 \\ a_2 & \cdots a_m & b_2 \\ a_2^2 & \cdots a_m^2 & b_3 \\ \cdot & \cdots \cdot & \cdot \\ a_2^{m-1} & \cdots a_m^{m-1} & b_m \end{vmatrix}.$$

The lemma now follows by induction.

It is to be remarked that if the characteristic of a field K is greater than m, each binary form of degree m with coefficients in K can be written as

$$b_1 x^m + m b_2 x^{m-1} y + \cdots + b_{m+1} y^m, \tag{3}$$

where the coefficient of $b_i x^{m-i+1} y^{i-1}$ is the binomial coefficient of $x^{m-i+1} y^{i-1}$ in the expansion of $(x+y)^m$.

3. **The range of the minimal number.**

We proceed with the following theorem in which $I(m)$ denotes the integer

$$\tfrac{1}{2} m [m(m-1) + 2]. \tag{4}$$

THEOREM 1. *For a field K with characteristic greater than m, and order at least $I(m)$, the minimal number of a binary form F does not exceed m.*

We write F as in (4). We exclude the trivial case $F\equiv 0$. If $b_1\neq 0$ while $b_i=0$ for $i>1$, the form F is simply b_1x^m, whence the minimal number of F is 1; similarly, if $b_{m+1}\neq 0$ while $b_i=0$ for $i<m+1$. If $m\geqq 2$ while b_1 and b_{m+1} are not zero, and if further $b_i=0$ for $i=2, 3, \cdots, m$, the form F is nonsingular in the sense of Oldenburger,[3] and has minimal number 2.

If F is of the first degree, the minimal number of F is clearly 1, while if F is quadratic, the minimal number is identical[4] with the rank of F and does not exceed 2.

It remains to consider forms F of degree at least 3 for which $b_2, \cdots, b_m$ are not all zero. It is no restriction to assume that $b_{m+1}\neq 0$. For if $b_{m+1}=0$, the form F can be transformed nonsingularly into a form with this property, as is clear from the following argument. We write $F=F(x, y)$. Since $F\not\equiv 0$, there exist values a and b of x and y respectively such that $F(a, b)\neq 0$. We make the transformation

$$x = x' + ay', \qquad y = x' + by',$$

on F to obtain a form $F'(x', y')$. Evidently, $F'(0, 1)=F(a, b)$.

We consider the following equality:

$$b_1x^m + mb_2x^{m-1}y + \cdots + b_{m+1}y^m = \sum_{i=1}^{m} \lambda_i(x + a_iy)^m. \tag{5}$$

The equality (5) is identically satisfied if the λ's and a's are chosen so that the following system of linear equations is valid:

$$\begin{aligned} \lambda_1 + \quad \lambda_2 + \cdots + \quad \lambda_m &= b_1, \\ a_1\lambda_1 + a_2\lambda_2 + \cdots + a_m\lambda_m &= b_2, \\ a_1^2\lambda_1 + a_2^2\lambda_2 + \cdots + a_m^2\lambda_m &= b_3, \\ \cdots\cdots\cdots\cdots\cdots\cdots &, \\ a_1^m\lambda_1 + a_2^m\lambda_2 + \cdots + a_m^m\lambda_m &= b_{m+1}. \end{aligned} \tag{6}$$

We shall prove that the a's can be chosen so that the rank of the matrix of coefficients of the λ's in (6) is m, while the rank of the augmented matrix is also m. The determinant of the augmented matrix of (6) is Δ. We write Δ as in (2).

In the expansion of M, the terms of lowest degree α in the a's are those which have b_{m+1} as coefficient. The degree α is explicitly

[3] R. Oldenburger, *Rational equivalence of a form to a sum of pth powers*, Transactions of this Society, vol. 44 (1938), pp. 219–249.

[4] M. Bôcher, *Introduction to Higher Algebra*, p. 135.

$\frac{1}{2}(m-1)(m-2)$. The terms of lowest degree, in the expansion of the polynomial a_iN for any i, are at least of degree $\alpha+1$. Thus the terms of degree α in the polynomial $M-a_iN$ [i in the range $2, 3, \cdots, m$] arise from M only, whence $M-a_iN$ is not identically zero in the a's. Thus the polynomial

$$(M - a_2N) \cdots (M - a_mN)N \tag{7}$$

of degree at most $I(m)-1$ is not identically zero in the a's. Evidently, $N\neq 0$ implies that $a_2, \cdots, a_m$ are distinct. Choose a set of values of $a_2, \cdots, a_m$ such that the polynomial (7) is different from zero. For this choice of the a's the polynomial $M-a_1N$ is linear in a_1, and $M-a_1N=0$ has a solution for a_1, distinct from $a_2, \cdots, a_m$. Thus there exist mutually distinct values of $a_1, a_2, \cdots, a_m$, such that $\Delta=0$. Since the a's are mutually distinct, the matrix of coefficients of the λ's in (6) has rank m. It follows that the augmented matrix has the same rank. It is well known that a system of linear equations has a solution if and only if the matrix of coefficients and the augmented matrix have the same rank.[5] Theorem 1 is now proved.

The following theorem was proved by Oldenburger.[6]

THEOREM 2. *For a field with characteristic greater than m, the minimal number of* $x^{m-1}y$ *is m.*

If the sum $\lambda_iL_i^m$ $(i=1, 2, \cdots, m)$ is chosen to be a minimal representation of $x^{m-1}y$, the sum

$$\lambda_1L_1^m + \cdots + \lambda_\rho L_\rho^m, \qquad \rho \leqq m,$$

is minimal. Thus for each ρ in the range $1, 2, \cdots, m$ there is a binary form of degree m with minimal number ρ. Applying Theorem 1 we have arrived at the following result.

THEOREM 3. *Let a field K be given as in Theorem* 1. *For the field K the range of the minimal numbers of binary forms of degree m is* $1, 2, \cdots, m$.

ARMOUR INSTITUTE OF TECHNOLOGY

[5] M. Bôcher, *Introduction to Higher Algebra*, p. 46.

[6] See first reference to Oldenburger above.