

# ON THE ZEROS OF POLYNOMIALS OVER DIVISION RINGS

BY

B. GORDON<sup>(1)</sup> AND T. S. MOTZKIN<sup>(2)</sup>

**1. Introduction.** Let  $f(x)$  be a polynomial of degree  $n$  with coefficients in the center  $K$  of a division ring  $D$ . Herstein [1] has shown that the number of zeros of  $f(x)$  in  $D$  is either  $\leq n$  or infinite. In this paper we investigate the situation for polynomials whose coefficients are in  $D$ , but not necessarily in  $K$ . Here one must distinguish between two types of polynomials, which we call *left* and *general*.

A left polynomial is an expression of the form  $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$ , where  $a_k \in D$  ( $k = 0, \dots, n$ ). Equality of two such polynomials is defined in the usual way. If  $a_0 \neq 0$ ,  $n$  is called the *degree* of  $f(x)$ . If  $c \in D$ , we define  $f(c) = a_0c^n + a_1c^{n-1} + \dots + a_n$ ; if  $f(c) = 0$ ,  $c$  is called a *zero* or *root* of  $f(x)$ . In §2 we prove that the number of distinct zeros of a left polynomial of degree  $n$  is either  $\leq n$  or infinite. This includes in particular a new proof of Herstein's result, avoiding the use of the Cartan-Brauer-Hua theorem.

Left polynomials can be added in the obvious way, and multiplied according to the rule  $(a_0x^m + \dots + a_m)(b_0x^n + \dots + b_n) = c_0x^{m+n} + \dots + c_{m+n}$ , where  $c_k = \sum_{i+j=k} a_i b_j$ ; they then form a ring  $D_L[x]$ . However, the specialization maps  $f(x) \rightarrow f(c)$  of  $D_L[x]$  onto  $D$  are not homomorphisms if  $c \notin K$ . To overcome this difficulty we are led to introduce *general polynomials*. Roughly speaking, a general polynomial is a sum of terms of the form  $a_0 x a_1 x \dots a_{k-1} x a_k$ , where  $a_0, \dots, a_k \in D$ . But there are certain identifications which must be made in order to obtain the various distributive laws, and to guarantee that  $cx = xc$  for  $c \in K$ ; therefore we now give a more careful description. Consider first the set  $S$  of all finite sequences  $(a_0, a_1, \dots, a_k)$ , where  $a_i \in D$ . It is easily seen that  $S$  forms a semigroup under the product

$$(a_0, a_1, \dots, a_k)(b_0, b_1, \dots, b_l) = (a_0, a_1, \dots, a_{k-1}, a_k b_0, b_1, \dots, b_l).$$

Let  $R$  be the semigroup ring of  $S$ , and let  $A_{ik}$  (where  $0 \leq i \leq k$ ) be the set of all elements in  $R$  of the form  $(a_0, \dots, a_i + b_i, \dots, a_k) - (a_0, \dots, a_i, \dots, a_k) - (a_0, \dots, b_i, \dots, a_k)$ . Let  $B_k$  be the set of all elements of  $R$  of the form

---

Presented to the Society, August 25, 1964 under the title *The number of zeros of a polynomial in a division ring*; received by the editors May 15, 1964.

<sup>(1)</sup> Alfred P. Sloan Fellow.

<sup>(2)</sup> National Science Foundation Grant GP 2480.

$(a_0, a_1, \dots, a_k) = (c_0 a_0, c_1 a_1, \dots, c_k a_k)$ , where  $c_0, \dots, c_k \in K$ , and  $c_0 c_1 \dots c_k = 1$ . We consider the quotient ring  $R/\mathfrak{a}$ , where  $\mathfrak{a}$  is the ideal generated by

$$\bigcup_{k=0}^{\infty} \left( \bigcup_{i=0}^k A_{ik} \cup B_k \right).$$

Each element  $(a_0)$  constitutes a residue class mod  $\mathfrak{a}$ , and these classes form a subring  $D'$  of  $R/\mathfrak{a}$  which is isomorphic to  $D$ . We now identify  $D'$  with  $D$ , and write  $a_0$  instead of  $(a_0)$ . Let  $x$  denote the residue class of  $(1, 1)$  mod  $\mathfrak{a}$ ; then it is easily verified that

$$(a_0, a_1, \dots, a_k) \equiv a_0 x a_1 x \dots a_{k-1} x a_k \pmod{\mathfrak{a}}.$$

The elements of  $R/\mathfrak{a}$  of the form  $a_0 x a_1 x \dots a_{k-1} x a_k$  are called *general monomials*, and denoted by symbols  $M(x)$ ,  $M_r(x)$ , etc. If  $a_0 a_1 \dots a_k \neq 0$ , then  $M(x) = a_0 x \dots x a_k$  is said to have degree  $k$ . Every element of  $R/\mathfrak{a}$  can be represented as a sum  $\sum_{r=1}^m M_r(x)$  of general monomials. Such elements are called *general polynomials*, and are denoted by symbols  $f(x)$ ,  $g(x)$ , etc. It can be shown that every  $f(x) \in R/\mathfrak{a}$  has a unique representation in the form  $f(x) = \sum_{r=1}^m M_r(x)$  where  $m$  is minimal. Then if  $f(x) \neq 0$ , we define its degree to be  $n = \max_r \deg M_r(x)$ .

We are now justified in introducing the notation  $D_G[x]$  for the ring  $R/\mathfrak{a}$ . There is a natural way of identifying  $D_L[x]$  with a subset of  $D_G[x]$ , but this subset is not a subring of  $D_G[x]$  unless  $D = K$ , in which case  $D_L[x] = D_G[x] = K[x]$ . It is, however, always possible to map  $D_G[x]$  homomorphically onto  $D_L[x]$  by extending the map  $a_0 x a_1 x \dots x a_k \rightarrow a_0 a_1 \dots a_k x^k$  to be additive.

In the construction of  $D_L[x]$  and  $D_G[x]$  we used only the fact that  $D$  was a ring with identity; hence we can define  $D_L[x_1, \dots, x_r]$  and  $D_G[x_1, \dots, x_r]$  by induction.

If  $c \in D$  and  $M(x) = a_0 x a_1 \dots x a_k$ , put  $M(c) = a_0 c a_1 \dots c a_k$ ; it is clear from the definition of  $\mathfrak{a}$  that  $M(c)$  depends only on the residue class mod  $\mathfrak{a}$  in which  $(a_0, \dots, a_k)$  lies, and is therefore well-defined. If  $f(x) = \sum M_r(x)$ , put  $f(c) = \sum M_r(c)$ ; this is also well-defined. The specializations  $f(x) \rightarrow f(c)$  are now homomorphisms of  $D_G[x]$  onto  $D$ .

An element  $c \in D$  is a *zero* or *root* of  $f(x) \in D_G[x]$  if  $f(c) = 0$ . Let  $N(f)$  be the number of distinct zeros of  $f(x)$ . In §3 we study  $N(f)$  in the case where  $K$  is infinite and  $[D:K] = d < \infty$ . We prove that if  $h$  is any integer in the range  $1 \leq h \leq n^d$ , then there is a polynomial  $f(x) \in D_G[x]$  of degree  $n$  such that  $N(f) = h$ .

**2. Left polynomials.** Our first two theorems are essentially due to Richardson [3]; however his proofs are not quite correct, as pointed out by Rohrbach [4].

**THEOREM 1.** *An element  $c \in D$  is a zero of a polynomial  $f(x) \in D_L[x]$  if and only if there exists a  $g(x) \in D_L[x]$  such that  $f(x) = g(x)(x - c)$ .*

**Proof.** Let  $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$ . The theorem is trivial if  $n = 0$  or  $1$ , so we may suppose  $n \geq 2$ . If  $c$  is a root of  $f(x)$ , let

$$g(x) = a_0x^{n-1} + (a_1 + a_0c)x^{n-2} + (a_2 + a_1c + a_0c^2)x^{n-3} \\ + \dots + (a_{n-1} + a_{n-2}c + \dots + a_0c^{n-1}).$$

Then a simple calculation shows that  $f(x) = g(x)(x - c)$ .

Conversely, suppose that  $f(x) = g(x)(x - c)$ , where  $g(x) = b_0x^{n-1} + b_1x^{n-2} + \dots + b_{n-1}$ . Equating coefficients, we obtain

$$a_0 = b_0, \\ a_1 = b_1 - b_0c, \\ a_2 = b_2 - b_1c, \\ \vdots \\ a_{n-1} = b_{n-1} - b_{n-2}c, \\ a_n = -b_{n-1}c.$$

Multiplying the equation for  $a_i$  on the right by  $c^{n-i}$  and adding, we get  $f(c) = 0$ . This completes the proof.

We note that the existence of a factorization  $f(x) = (x - c)h(x)$  neither implies nor is implied by  $f(c) = 0$ .

Now let  $D^*$  be the multiplicative group of nonzero elements of  $D$ . Two elements  $a, b \in D$  are called conjugates if  $a = bbt^{-1}$  for some  $t \in D^*$ . As usual this equivalence relation partitions  $D$  into disjoint sets called conjugacy classes.

**THEOREM 2.** *If  $f(x) \in D_L[x]$  has degree  $n$ , then at most  $n$  conjugacy classes of  $D$  contain roots of  $f(x)$ .*

**Proof.** The proof is by induction on  $n$ . It is clear that a polynomial of degree zero has no roots, and a polynomial of degree one has exactly one root. Hence the theorem is true for  $n < 2$ . Now suppose  $n \geq 2$ , and assume that the theorem has already been proved for polynomials of degree  $< n$ . Suppose  $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$  has  $n + 1$  distinct zeros  $c_0, c_1, \dots, c_n$ . By Theorem 1 we have factorizations  $f(x) = g_i(x)(x - c_i)$  ( $i = 0, \dots, n$ ). Now assume  $i > 0$ , and set  $t_i = c_i - c_0$ . Then  $x - c_0 = x - c_i + t_i$ ; hence

$$g_i(x)(x - c_i) = g_0(x)(x - c_0) \\ = g_0(x)(x - c_i) + g_0(x)t_i.$$

Thus

$$g_0(x) = [g_i(x) - g_0(x)](x - c_i)t_i^{-1} \\ = [g_i(x) - g_0(x)]t_i^{-1}(x - t_it_it_i^{-1}),$$

remembering that  $xt_i^{-1} = t_i^{-1}x$  in the ring  $D_L[x]$ . Another application of Theorem 1 now shows that  $t_i c_i t_i^{-1}$  is a root of  $g_0(x)$  ( $i = 1, \dots, n$ ). Since  $\deg g_0(x) < n$ , the induction hypothesis implies that two of the elements  $t_i c_i t_i^{-1}$  are conjugate (they may be equal). But if, say,  $t_1 c_1 t_1^{-1}$  is conjugate to  $t_2 c_2 t_2^{-1}$ , then  $c_1$  is conjugate to  $c_2$ , completing the induction.

**THEOREM 3.** *If  $D$  is a noncommutative division ring, then the centralizer  $Z(c)$  of any element  $c \in D$  is infinite.*

**Proof.** We suppose  $Z(c)$  is finite, and obtain a contradiction as follows. The center  $K$  of  $D$  is contained in  $Z(c)$ , so  $K$  is a finite field; say  $K = \text{GF}(q)$ . If  $c \in K$ , then  $Z(c) = D$ , which is infinite by Wedderburn's theorem. Hence  $c \notin K$ . Another application of Wedderburn's theorem shows that  $Z(c)$  is a field, and hence  $Z(c) = \text{GF}(q^f)$ , where  $f > 1$ . The mapping  $\mu: a \rightarrow a^q$  is an automorphism of  $Z(c)$  with fixed field  $K$ . By a well-known theorem [2, p. 162],  $\mu$  can be extended to an inner automorphism of  $D$ . Thus there is an element  $t \in D$  such that  $tat^{-1} = a^q$  for all  $a \in Z(c)$ . In particular  $tct^{-1} = c^q$ , and by iteration,  $t^f c t^{-f} = c^{q^f} = c$ . Hence  $t^f \in Z(c)$ , which implies that  $t$  is of finite order. From these facts it follows easily that there are only a finite number of distinct elements of the form  $\sum \lambda_{i,j} c^i t^j$  ( $\lambda_{i,j} \in K$ ) and that they form a subring  $E \subset D$ . The nonzero elements of  $E$  form a finite semigroup  $E^* \subset D^*$ ; hence  $E^*$  is a group, and  $E$  is a division ring. This contradicts Wedderburn's theorem, since  $tc = c^q t \neq ct$ .

**THEOREM 4.** *If a polynomial  $f(x) \in D_L[x]$  has two distinct zeros in a conjugacy class of  $D$ , then it has infinitely many zeros in that class.*

**Proof.** Suppose  $c$  and  $tct^{-1} \neq c$  are zeros of  $f(x) = a_0 x^n + \dots + a_n$ . Consider the equation

$$(1) \quad f(ycy^{-1}) = a_0 y c^n y^{-1} + a_1 y c^{n-1} y^{-1} + \dots + a_n = 0,$$

where  $y$  is the unknown. Except for the extraneous root 0, this is equivalent to the equation

$$(2) \quad a_0 y c^n + a_1 y c^{n-1} + \dots + a_n y = 0.$$

By hypothesis  $y = 1$  and  $y = t$  are solutions of (2). Now (2) clearly has the following properties:

- (i) If  $y_1$  and  $y_2$  are solutions, so is  $y_1 + y_2$ .
- (ii) If  $y$  is a solution and  $z \in Z(c)$ , then  $yz$  is a solution.

Combining these properties we see that  $t + z$  is a solution of (2) for any  $z \in Z(c)$ . Moreover  $t + z \neq 0$  since  $t \notin Z(c)$ . Hence  $t + z$  is a solution of (1), and so  $(t + z)c(t + z)^{-1}$  is a zero of  $f(x)$ . To complete the proof we show that the elements  $(t + z)c(t + z)^{-1}$  are all distinct and apply Theorem 3. Suppose that  $(t + z_1)c(t + z_1)^{-1} = (t + z_2)c(t + z_2)^{-1}$ , where  $z_1, z_2 \in Z(c)$ . Then  $(t + z_2)^{-1}(t + z_1)$  commutes with  $c$ , so that  $(t + z_2)^{-1}(t + z_1) = z_3$  where  $z_3 \in Z(c)$ . Thus  $t + z_1 = (t + z_2)z_3 = tz_3 + z_2z_3$ . If  $z_3 \neq 1$ , this

implies that  $t = (z_2z_3 - z_1)(1 - z_3)^{-1}$ , which is in  $Z(c)$  since  $Z(c)$  is a division ring. This contradicts the fact that  $tct^{-1} \neq c$ . Hence  $z_3 = 1$ , which means that  $t + z_1 = t + z_2$ , or finally  $z_1 = z_2$ .

**THEOREM 5.** *If  $f(x) \in D_L[x]$  has degree  $n$ , then the number of zeros of  $f(x)$  is either  $\leq n$  or infinite.*

**Proof.** If  $f(x)$  has more than  $n$  zeros, then two of them lie in the same conjugacy class by Theorem 2. By Theorem 4, this class contains infinitely many zeros of  $f(x)$ .

**3. General polynomials.** We suppose throughout this section that  $[D:K] = d < \infty$ . Elements of  $K$  are denoted by greek letters. Let  $1 = e_1, \dots, e_d$  be a basis of  $D$  over  $K$ , and let  $x = \xi_1e_1 + \dots + \xi_de_d$  be the generic element of  $D$ . If  $f(x)$  is a general polynomial of degree  $n$ , we can express all its coefficients in terms of the basis  $e_1, \dots, e_d$ . Then after multiplying the factors of each monomial  $a_0xa_1 \dots xa_k$  and collecting terms, we obtain

$$f(x) = f_1(\xi_1, \dots, \xi_d)e_1 + \dots + f_d(\xi_1, \dots, \xi_d)e_d,$$

where the  $f_i(\xi_1, \dots, \xi_d)$  are polynomials in  $K[\xi_1, \dots, \xi_d]$ . Thus the equation  $f(x) = 0$  is equivalent to the system  $f_i(\xi_1, \dots, \xi_d) = 0$  ( $i = 1, \dots, d$ ). We note that each  $f_i$  is either identically zero or of degree  $\leq n$ .

To avoid endless separation of cases in what follows, we make the convention that 0 is a homogeneous polynomial of degree  $n$  for any  $n \geq 0$ .

**THEOREM 6.** *If  $f_i(\xi_1, \dots, \xi_d) \in K[\xi_1, \dots, \xi_d]$  ( $i = 1, \dots, d$ ) are  $d$  given polynomials of degree  $\leq n$ , then there exists a polynomial  $f(x) \in D_G[x]$  of degree  $\leq n$  such that  $f(x) = \sum_{i=1}^d f_i e_i$ .*

**Proof.** The theorem is clearly true if  $d = 1$ , i.e.,  $D = K$ . Assume from now on that  $d > 1$ , so that  $D$  is noncommutative. It suffices to show that if the  $f_i$  are all homogeneous polynomials of degree  $n$ , then there is a homogeneous polynomial  $f(x) \in D_G[x]$  of degree  $n$  with  $f(x) = \sum_{i=1}^d f_i e_i$ . (The general case then follows by forming sums.) If  $n = 0$  the result is obvious. If  $n = 1$ , we have  $f_i(\xi_1, \dots, \xi_d) = \sum_{j=1}^d \alpha_{ij} \xi_j$  with  $\alpha_{ij} \in K$ . Thus the  $f_i$  define a linear transformation of  $D$ , considered as a vector space over  $K$ , into itself. It is our object to show that this transformation is of the form  $x \rightarrow f(x)$  for some homogeneous polynomial  $f(x) \in D_G[x]$  of degree one. Such polynomials have the form  $f(x) = \sum a_j x b_j$ , where  $a_j, b_j \in D$ . From this it is trivial to verify that the corresponding transformations  $x \rightarrow f(x)$  form a ring  $R$ . We now show that  $R$  is doubly transitive. Let  $a$  and  $b$  be two elements of  $D$  which are linearly independent over  $K$ , and let  $c, d$  be any two elements of  $D$ . Then  $ab \neq 0$ , and  $ab^{-1} \notin K$ . Hence there is an element  $r \in D$  such that  $s = rab^{-1} - ab^{-1}r \neq 0$ . Then  $t = ba^{-1}r^{-1} - r^{-1}ba^{-1} \neq 0$ . The polynomial

$$g(x) = (rx b^{-1} - x b^{-1}r) s^{-1}c + (x a^{-1}r^{-1} - r^{-1}x a^{-1}) t^{-1}d$$

satisfies  $g(a) = c$  and  $g(b) = d$ , proving that  $R$  is doubly transitive. By a theorem of Jacobson [2, p. 32],  $R$  is the ring of all linear transformations of  $D$ ; thus there is an  $f(x) \in D_G[x]$  such that  $f(x) = \sum_{i=1}^d f_i e_i$ .

To deal with the case  $n > 1$  we consider the ring  $D_G[x_1, \dots, x_n]$  of general polynomials in  $n$  indeterminates. A polynomial  $p(x_1, \dots, x_n) \in D_G[x_1, \dots, x_n]$  is called a *multilinear form* if it is homogeneous and linear in each indeterminate  $x_k$ . Putting  $x_k = \sum_{i=1}^d \xi_i^{(k)} e_i$ , and expressing the coefficients of  $f$  in terms of the basis  $e_1, \dots, e_d$ , we find that

$$p(x_1, \dots, x_n) = \sum_{i=1}^d p_i(\xi_1^{(1)}, \dots, \xi_d^{(n)}) e_i,$$

where the  $p_i$  are polynomials in  $K[\xi_1^{(1)}, \dots, \xi_d^{(n)}]$ . Moreover  $p$  is multilinear if and only if all the  $p_i$  are multilinear (i.e., linear in each set of indeterminates  $\xi_1^{(k)}, \dots, \xi_d^{(k)}$ ). We assert that given any  $d$  multilinear forms  $p_i \in K[\xi_1^{(1)}, \dots, \xi_d^{(n)}]$ , there exists a multilinear form  $p \in D_G[x_1, \dots, x_n]$  such that  $p = \sum f_i e_i$ . For let

$$g_k(\xi_1^{(k)}, \dots, \xi_d^{(k)}) \in K[\xi_1^{(k)}, \dots, \xi_d^{(k)}] \quad (k = 1, \dots, n)$$

be given linear forms. By what we have already shown there exist polynomials  $h_k(x_k) \in D_G[x_k]$  ( $k = 1, \dots, n$ ) such that  $h_1(x_1) = g_1 e_i$ , and  $h_k(x_k) = g_k e_1$  for  $k > 1$ . Then (recalling that  $e_1 = 1$ ) we have  $h_1(x_1) \cdots h_n(x_n) = g_1 \cdots g_n e_i$ . The terms of the given polynomial  $p_i$  are of the form  $g_1 \cdots g_n$ , so  $p_i$  is a sum of such polynomials. Hence  $p_i e_i$  is the sum of the corresponding polynomials  $h_1(x_1) \cdots h_n(x_n) \in D_G[x_1, \dots, x_n]$ . Applying this fact for each  $i = 1, \dots, d$  and summing over  $i$  we obtain a multilinear form  $p(x_1, \dots, x_n) \in D_G[x_1, \dots, x_n]$  such that  $p = \sum p_i e_i$ .

Now suppose that

$$f_i(\xi_1, \dots, \xi_d) \in K[\xi_1, \dots, \xi_d] \quad (i = 1, \dots, d)$$

are  $d$  given homogeneous polynomials of degree  $n$ . By "polarization" we construct multilinear polynomials  $p_i(\xi_1^{(1)}, \dots, \xi_d^{(n)}) \in K[\xi_1^{(1)}, \dots, \xi_d^{(n)}]$  such that  $p_i$  reduces to  $f_i$  under the substitution  $\xi_1^{(1)} = \dots = \xi_1^{(n)} = \xi_1, \dots, \xi_d^{(1)} = \dots = \xi_d^{(n)} = \xi_d$ . By what we have shown, there is a polynomial  $p(x_1, \dots, x_n) \in D_G[x_1, \dots, x_n]$  such that  $p = \sum p_i e_i$ . Then  $f(x) = p(x, \dots, x) \in D_G[x]$  satisfies  $f = \sum f_i e_i$ , completing the proof.

**THEOREM 7.** *Let  $K$  be any infinite field, and let  $\{n_1, n_2, \dots, n_d\}$  be any set of positive integers. Suppose  $1 \leq h \leq n_1 n_2 \cdots n_d$ . Then there exist  $d$  polynomials  $f_i(\xi_1, \dots, \xi_d) \in K[\xi_1, \dots, \xi_d]$  ( $i = 1, \dots, d$ ) such that  $\deg f_i = n_i$ , and such that the system  $f_i(\xi_1, \dots, \xi_d) = 0$  ( $i = 1, \dots, d$ ) has exactly  $h$  solutions. The same conclusion holds for  $h = 0$ , provided that  $d > 1$ .*

**Proof.** It is convenient to prove a stronger statement, namely that the  $f_i$  can be chosen so that  $f_i$  is a product of  $n_i$  linear polynomials, and such that if  $p_i$  is any linear factor of  $f_i$  ( $i = 1, \dots, d$ ), then  $p_1, \dots, p_d$  are linearly

independent over  $K$ . Consider first the case  $d = 1$ , and write  $n_1 = n$ ,  $\xi_1 = \xi$ . We have  $0 \leq h \leq n$ . Since  $K$  is infinite, there exist  $h$  distinct elements  $\alpha_1, \dots, \alpha_h \in K$ . The polynomial  $f(\xi) = (\xi - \alpha_1)^{n-h+1}(\xi - \alpha_2) \cdots (\xi - \alpha_h)$  clearly does what is required.

Assume next that  $d > 1$ , and that  $n_1 = n_2 = \dots = n_d = 1$ . Then  $0 \leq h \leq 1$ . If  $h = 1$ , set  $f_i = \xi_i$ , for all  $i$ . If  $h = 0$  put  $f_1 = \xi_1$ ,  $f_2 = \xi_1 + 1$ , and  $f_i = \xi_i$  for all  $i > 2$ . (Note that these polynomials are linearly independent over  $K$ .) The proof now proceeds by induction on  $d$ , and for fixed  $d$  by induction on  $s = \sum_{i=1}^d n_i$ . Assume then that  $s > d$ , and that the theorem is true for all sets  $\{m_1, \dots, m_c\}$ , where  $c < d$ , and also for all sets  $\{m_1, \dots, m_d\}$ , where  $\sum_{i=1}^d m_i < s$ . Suppose without loss of generality that  $n_1 > 1$ . Then the induction hypothesis can be applied to the set  $\{n_1 - 1, n_2, \dots, n_d\}$ . Thus for any  $h$  in the range  $0 \leq h \leq (n_1 - 1)n_2 \cdots n_d$  we can find polynomials  $g_i(\xi_1, \dots, \xi_d)$  ( $i = 1, \dots, d$ ) of the special type described above, such that  $\deg g_1 = n_1 - 1$ ,  $\deg g_i = n_i$  for  $i > 1$ , and such that the system  $g_i(\xi_1, \dots, \xi_d) = 0$  has exactly  $h$  solutions. Let  $p(\xi_1, \dots, \xi_d)$  be one of the linear factors of  $g_1(\xi_1, \dots, \xi_d)$ . Then set  $f_1 = pg_1$  and  $f_i = g_i$  for  $i > 1$ . Clearly the polynomials  $f_i$  have the desired property.

We may therefore suppose that  $(n_1 - 1)n_2 \cdots n_d < h \leq n_1 n_2 \cdots n_d$ . Write  $h = (n_1 - 1)n_2 \cdots n_d + k$ , where  $1 \leq k \leq n_2 \cdots n_d$ . By induction there exist polynomials  $g_i \in K[\xi_2, \dots, \xi_d]$  ( $i = 2, \dots, d$ ) of our special type such that  $\deg g_i = n_i$ , and such that the system  $g_i(\xi_2, \dots, \xi_d) = 0$  ( $i = 2, \dots, d$ ) has exactly  $k$  solutions. Let the decomposition of  $g_i$  into linear factors be  $g_i = p_i^{(1)} \cdots p_i^{(n_i)}$  ( $i = 2, \dots, d$ ). Set  $f_i = \prod_{j=1}^{n_i} (\alpha_{ij} \xi_1 + p_i^{(j)})$  ( $i = 2, \dots, d$ ), where the  $\alpha_{ij}$  are elements in  $K$  which will be specified later. Put

$$f_1 = \xi_1 \prod_{j=2}^{n_1} (\beta_j \xi_1 + p_1^{(j)}),$$

where the  $\beta_j$  are elements of  $K$  to be specified later, and the  $p_1^{(j)}$  are linear polynomials in  $\xi_2, \dots, \xi_d$ , to be determined. There is no nontrivial relation of the form

$$\lambda_1 \xi_1 + \lambda_2 (\alpha_{2r} \xi_1 + p_2^{(r)}) + \dots + \lambda_d (\alpha_{d1} \xi_1 + p_d^{(t)}) = 0.$$

For setting  $\xi_1 = 0$  we see that  $\lambda_2 = \dots = \lambda_d = 0$  by the independence of  $p_2^{(r)}, \dots, p_d^{(t)}$ . Hence  $\lambda_1 = 0$ . Now choose the polynomials  $p_1^{(j)}$  ( $j > 1$ ) so that  $p_1^{(j)}, p_2^{(r)}, \dots, p_d^{(t)}$  are linearly independent for all choices of  $j, r, \dots, t$ . This can be done since the set  $V$  of linear polynomials in  $\xi_2, \dots, \xi_d$  is a  $d$ -dimensional vector space over the infinite field  $K$ , and we need merely avoid a finite number of  $(d - 1)$ -dimensional subspaces of  $V$  in choosing the  $p_1^{(j)}$ . Then it is clear that  $\beta_j \xi_1 + p_1^{(j)}, \alpha_{2r} \xi_1 + p_2^{(r)}, \dots, \alpha_{d1} \xi_1 + p_d^{(t)}$  are linearly independent. Furthermore the  $d \times (d - 1)$  matrix formed by the coefficients of  $\xi_2, \dots, \xi_d$  in the polynomials  $p_1^{(j)}, p_2^{(r)}, \dots, p_d^{(t)}$  has rank  $d - 1$ . Hence

by avoiding a finite number of proper subspaces in the space  $W$  of vectors whose coordinates are the  $\beta_j$  and  $\alpha_{ij}$ , we can choose the  $\alpha$ 's and  $\beta$ 's so that the matrix formed by the coefficients of  $\xi_1, \dots, \xi_d$  in the polynomials  $\beta_j \xi_1 + p_1^{(j)}, \alpha_{2r} \xi_1 + p_2^{(r)}, \dots, \alpha_{dt} \xi_1 + p_d^{(t)}$  is nonsingular for all choices of  $j > 1, r, \dots, t$ . Then the system  $\beta_j \xi_1 + p_1^{(j)} = \alpha_{2r} \xi_1 + p_2^{(r)} = \dots = \alpha_{dt} \xi_1 + p_d^{(t)} = 0$  has a unique solution for each  $j > 1, r, \dots, t$ . By avoiding a further finite set of subspaces of  $W$ , we can insure that no  $d + 1$  of these equations have a common solution, so that the solutions corresponding to different choices of  $j, r, \dots, t$  are distinct.

Now consider the system  $f_i(\xi_1, \dots, \xi_d) = 0$  ( $i = 1, \dots, d$ ). For this to be satisfied, some linear factor of each  $f_i$  must vanish. If  $\xi_1 = 0$ , then the system reduces to  $g_i(\xi_2, \dots, \xi_d) = 0$  ( $i = 2, \dots, d$ ). This has  $k$  solutions by the construction of the  $g_i$ . If  $\xi_1 \neq 0$ , we get exactly one solution for every choice of a linear factor from each of the polynomials  $f_1, \dots, f_d$ . There are  $(n_1 - 1)n_2 \dots n_d$  such choices, and therefore the total number of solutions is  $k + (n_1 - 1)n_2 \dots n_d = h$ . This completes the proof.

**THEOREM 8.** *Let  $D$  be a noncommutative division ring with  $[D:K] = d < \infty$ . Suppose  $n \geq 1$ , and let  $h$  be an integer satisfying  $0 \leq h \leq n^d$ . Then there is a polynomial  $f(x) \in D_G[x]$  of degree  $n$  with  $N(f) = h$ .*

**Proof.** By Theorem 7 with  $n_1 = \dots = n_d = n$ , we can find  $d$  polynomials  $f_i(\xi_1, \dots, \xi_d) \in K[\xi_1, \dots, \xi_d]$  of degree  $n$  such that the system  $f_i(\xi_1, \dots, \xi_d) = 0$  ( $i = 1, \dots, d$ ) has exactly  $h$  solutions. By Theorem 6 there is a polynomial  $f(x) \in D_G[x]$  of degree  $\leq n$  such that  $f(x) = \sum_{i=1}^d f_i e_i$ . Clearly  $\deg f = n$ , and  $N(f) = h$ .

The question of what values  $> n^d$ , if any, can be assumed by  $N(f)$  for polynomials  $f(x) \in D_G[x]$  of degree  $n$ , is extremely deep, and depends on the arithmetic nature of  $K$ . By Bézout's theorem we know that if  $n^d < N(f) < \infty$ , then the system  $f_i(\xi_1, \dots, \xi_d) = 0$  has infinitely many solutions in the algebraic closure  $\bar{K}$ . But of course  $K \neq \bar{K}$ , since there are no division rings of finite dimension  $d > 1$  over an algebraically closed field. Thus we gain little information about the zeros of the system  $f_i = 0$  in  $K$ .

For example, let  $K = \mathbf{Q}(\sqrt{-3})$ , where  $\mathbf{Q}$  is the rational field. Let  $D$  be a division ring with center  $K$  such that  $[D:K] = 4$ . Then the polynomial

$$f(x) = (\xi_3 - \xi_2^2)e_1 + (\xi_2 \xi_3 - 3\xi_1^2 - 3\xi_1 - 1)e_2 + (\xi_4^2 - 1)e_3$$

has degree 2, but has exactly 18 zeros in  $D$ . To see this, we consider the system

$$\begin{aligned} \xi_3 &= \xi_2^2, \\ \xi_2 \xi_3 &= 3\xi_1^2 + 3\xi_1 + 1, \\ \xi_4^2 &= 1. \end{aligned}$$



Eliminating  $\xi_3$  from the first two equations we obtain

$$\xi_2^3 = 3\xi_1^2 + 3\xi_1 + 1 = (\xi_1 + 1)^3 - \xi_1^3.$$

By Fermat's last theorem for cubes, the only solutions in  $\mathbb{Q}(\sqrt{-3})$  are such that  $\xi_2 = 0$  or  $\xi_1 + 1 = 0$  or  $\xi_1 = 0$ . There are nine such solutions. Once  $\xi_1, \xi_2$  are known,  $\xi_3$  is uniquely determined, and  $\xi_4 = \pm 1$ . Hence our system has precisely eighteen solutions in  $K$ , as asserted. On the other hand,  $n^d = 2^4 = 16$ .

#### REFERENCES

1. I. N. Herstein, *Conjugates in division rings*, Proc. Amer. Math. Soc. 7 (1956), 1021-1022.
2. N. Jacobson, *Structure of rings*, Amer. Math. Soc. Colloq. Publ. Vol. 37, Amer. Math. Soc., Providence, R. I., 1956.
3. A. R. Richardson, *Equations over a division algebra*, Messenger of Mathematics 57 (1927), 1-6.
4. H. Rohrbach, Review of paper [3], Jahrbuch über die Fortschritte der Mathematik 53 (1927), 122.

UNIVERSITY OF CALIFORNIA,  
LOS ANGELES, CALIFORNIA