It remains only to prove that each of the numbers θ, ϕ given by Lemma 1 is either a T-number or an S-number of type exceeding Θ. From Lemma 3 we obtain

$$\max(|\theta-\Theta_0^{(n)}|, |\phi-\Phi_0^{(n)}|) < 6^{7(n+1)} H_n^{-3\Theta-1/2},$$

and it follows that θ, ϕ cannot be S-numbers of type $\leqslant \Theta$ (6). Finally we appeal to Theorem 1 of [1]. From Lemma 4 and the inequality

$$H_{n+1} < H_{n-1}^{100\Theta^2}(6e^{\eta})^{6+27\Theta}$$

it follows that all the hypotheses of Theorem 1 are satisfied with $a_j = \Theta_0^{(2j)}$, or $a_j = \Phi_0^{(2j)}$, provided j is sufficiently large (and similarly with the superscript $2j+1$ in place of $2j$), and hence θ, ϕ are neither algebraic nor U-numbers. This completes the proof of the theorem.

(6) See Schneider [9], Satz 22, p. 82. Again we are assuming δ_2 sufficiently small so that $H_n^{1/2} > 6^{7(n+1)}$ if n is sufficiently large.

References

[1] A. Baker, *On Mahler's classification of transcendental numbers*, Acta Math. 111 (1964), pp. 97-120.

[2] J. W. S. Cassels, *Simultaneous Diophantine approximation*, Proc. London Math. Soc. 5 (1955), pp. 435-448.

[3] — *On a result of Marshall Hall*, Mathematika 3 (1956), pp. 109-110.

[4] — *An introduction to the geometry of numbers*, Berlin, Göttingen, Heidelberg, 1959.

[5] H. Davenport, *Simultaneous Diophantine approximation*, Mathematika 1 (1954), pp. 51-72.

[6] — *A note on Diophantine approximation*, Studies in mathematical analysis and related topics, Stanford University Press, 1962, pp. 77-81.

[7] — *A note on Diophantine approximation* (II), Mathematika 11 (1964), pp. 50-58.

[8] W. M. Schmidt, *On badly approximable numbers*, Mathematika 12 (1965), pp. 10-20.

[9] Th. Schneider, *Einführung in die transzendenten Zahlen*, Berlin, Göttingen, Heidelberg, 1957.

Reçu par la Rédaction le 4. 4. 1966

ACTA ARITHMETICA
XII (1967)

On a conjecture of Davenport and Lewis concerning exceptional polynomials*

by

C. R. MacCluer (Ann Arbor, Mich.)

1. Exceptional polynomials over arbitrary fields. Let K be an arbitrary field. A polynomial $f(x)$ in $K[x]$ is said to be *exceptional over* K if the polynomial $\Phi(x, y) = (f(x)-f(y))/(x-y)$ has no absolutely irreducible factors in $K[x, y]$.

In the investigation into the average error term of the number of solutions of congruence relations, Davenport and Lewis [1] were led to propose the following conjecture:

The Davenport-Lewis Conjecture. *For $f(x)$ in $Z[x]$ and for all large primes p, if $f(x)$ is exceptional over Z_p, then the map*

$$f\colon Z_p \to Z_p$$

is one-to-one and onto.

The object of this note is to show that the Davenport-Lewis Conjecture is indeed correct. In fact,

Theorem 1. *Let K be an arbitrary field and let $f(x)$ be a polynomial in the ring $K[x]$ of degree n. Suppose* $\operatorname{char} K = 0$ *or* $n < \operatorname{char} K$. *If $f(x)$ is exceptional over K, then $f(x)$ is a one-to-one map of K into K.*

The proof of Theorem 1 will follow some necessary observations concerning the splitting fields of polynomials in two variables and some remarks on pure equations.

For the remainder of this note let K be an arbitrary field and let A be the algebraic closure of K.

Definition 1. If $a(x, y)$ in $K[x, y]$ is of the form

$$a(x, y) = ax^n + P_1(y)x^{n-1} + \ldots + P_n(y)$$

where each $P_i(y)$ is in $K[y]$ and where a is a non-zero element of K, then $a(x, y)$ is said to be *regular in* x. If, in addition, $a = 1$, then $a(x, y)$ is said to be *monic in* x.

* Research was sponsored by the National Science Foundation. Ann Arbor, Michigan, U. S. A.

DEFINITION 2. Suppose $\alpha(x, y)$ in $K[x, y]$ is regular in x. If Σ is a finite normal extension of K such that $\alpha(x, y)$ factors into a product of absolutely irreducible factors in $\Sigma[x, y]$, then Σ is said to be a *splitting field for* $\alpha(x, y)$ *over* K.

Remark. Clearly every regular polynomial has at least one splitting field over K.

All splitting fields over K are to be thought of as subfields of A. With this in mind we have the following:

LEMMA A. *Suppose* $\alpha(x, y)$ *in* $K[x, y]$ *is regular in* x. *Then the intersection of all splitting fields for* $\alpha(x, y)$ *over* K *is a splitting field for* $\alpha(x, y)$ *over* K *denoted by* $\Sigma_K(\alpha)$.

Proof. Choose a in K such that $a\alpha(x, y)$ is monic in x. Let

$$a\alpha(x, y) = \alpha_1(x, y)\dots\alpha_r(x, y)$$

where each $\alpha_i(x, y)$ is irreducible in $A[x, y]$ and monic in x. Let $\Sigma_K(\alpha) = K(c_1, \dots, c_k)$ where $c_1, \dots, c_k$ are the coefficients of the terms of $\alpha_1(x, y), \dots, \alpha_r(x, y)$. Then since isomorphisms of $\Sigma_K(\alpha)$ over K map factors of $\alpha(x, y)$ onto factors of $\alpha(x, y)$, we see that $\Sigma_K(\alpha)$ is normal over K. Therefore $\Sigma_K(\alpha)$ is a splitting field for $\alpha(x, y)$ over K.

Let Σ be a splitting field for $\alpha(x, y)$ over K. Then since irreducible factors of $\alpha(x, y)$ in $\Sigma[x, y]$ are absolutely irreducible and may be chosen monic in x, we see that these factors must coincide with the factors $\alpha_1(x, y), \dots, \alpha_r(x, y)$ in $A[x, y]$. Therefore Σ contains the coefficients $c_1, \dots, c_k$ and hence contains $\Sigma_K(\alpha)$. This proves Lemma A.

LEMMA B. *Let* $\beta(x, y)$ *be irreducible in the ring* $K[x, y]$ *and monic in* x. *Then the irreducible factors of* $\beta(x, y)$ *in* $\Sigma_K(\beta)[x, y]$ *that are monic in* x *are conjugate over* K. *That is, if* $\beta_1(x, y)$ *and* $\beta_2(x, y)$ *are irreducible in* $\Sigma_K(\beta)[x, y]$, *monic in* x, *and divide* $\beta(x, y)$, *then there is an automorphism of* $\Sigma_K(\beta)$ *fixing* K *that maps* $\beta_1(x, y)$ *onto* $\beta_2(x, y)$.

Proof. Let Ω be the elements of $\Sigma_K(\beta)$ that are separable over K. Then Ω is normal over K. Let

$$\beta(x, y) = \beta_1(x, y)\dots\beta_r(x, y)$$

where each $\beta_i(x, y)$ is monic in x and irreducible in $\Omega[x, y]$. Let G be the galois group of Ω over K. Then G permutes the factors $\beta_i(x, y)$ among themselves. But the product of the factors in an orbit of G is a polynomial with coefficients in K that divides $\beta(x, y)$. Therefore since $\beta(x, y)$ is irreducible in $K[x, y]$, there can be only one orbit. This would complete the proof if $\Sigma_K(\beta)$ were a separable extension of K, since in that case, $\Omega = \Sigma_K(\beta)$.

Assume that $\Omega \neq \Sigma_K(\beta)$. Then some $\beta_i(x, y)$, say for $i = 1$, must factor further in $\Sigma_K(\beta)[x, y]$; otherwise Ω would be a splitting field for $\beta(x, y)$ over K which contradicts the minimality of $\Sigma_K(\beta)$. Let

$$\beta_1(x, y) = \beta_{11}(x, y)\dots\beta_{1s}(x, y)$$

where each $\beta_{1i}(x, y)$ is irreducible in $\Sigma_K(\beta)[x, y]$ and monic in x.

Then, by assumption, $s > 1$. Let $p = \operatorname{char} K$ and let e be the exponent of the purely inseparable extension $\Sigma_K(\beta)/\Omega$. Then each polynomial $\beta_{1j}(x, y)^{p^e}$ has coefficients in Ω. But we have

$$\beta_1(x, y)^{p^e} = \beta_{11}(x, y)^{p^e}\dots\beta_{1s}(x, y)^{p^e}.$$

Therefore, because of the unique factorization property of the rings $\Omega[x, y]$ and $\Sigma_K(\beta)[x, y]$, the $\beta_{1i}(x, y)$ coincide; i.e.,

$$\beta_1(x, y) = \beta_{11}(x, y)^s.$$

Since every automorphism of Ω over K may be extended in one and only one way to an automorphism of $\Sigma_K(\beta)$ over K, we see that the (absolutely) irreducible factors of $\beta(x, y)$ in $\Sigma_K(\beta)[x, y]$ that are monic in x are conjugate. To be explicit, let σ_i be an automorphism of $\Sigma_K(\beta)$ over K that sends $\beta_1(x, y)$ into $\beta_i(x, y)$. Then set $\beta_{i1}(x, y) = \beta_{11}(x, y)^{\sigma_i}$. Then the factorization of $\beta(x, y)$ proceeds in the steps:

(over K)	$\beta(x, y)$
(over Ω)	$\beta_1(x, y)\dots\beta_r(x, y)$
(over $\Sigma_K(\beta)$)	$\beta_{11}(x, y)^s\dots\beta_{r1}(x, y)^s$.

This proves Lemma B.

Remark. The proof of Lemma B shows in particular that if $\Sigma_K(\beta)$ contains elements inseparable over K, then $\beta(x, y)$ necessarily has repeated factors.

It is possible to locate the minimal splitting field for a large class of polynomials regular in x by the following Lemma:

LEMMA C. *Let* $\alpha(x, y)$ *in* $K[x, y]$ *be regular in* x *and let* $F(x, y)$ *be the homogeneous term of* $\alpha(x, y)$ *of largest homogeneous degree. Then for each element* a *of* K *such that* $F(x, a)$ *has no double roots,* $\Sigma_K(\alpha)$ *is a subfield of the splitting field of the polynomial* $g(x) = F(x, a)$ *over* K.

Proof. Let a be an element of K such that $F(x, a)$ has no double roots. Let Ω be the splitting field of the polynomial $g(x) = F(x, a)$ over K. Choose c in K such that $c\alpha(x, y)$ is monic in x. Let

$$c\alpha(x, y) = \alpha_1(x, y)\dots\alpha_r(x, y)$$

where each $a_i(x, y)$ is irreducible in $\Omega[x, y]$ and monic in x. Let Λ be the smallest normal extension of Ω that contains $\Sigma_K(a)$. Hence Λ is a splitting field for $a(x, y)$ over Ω since Λ contains a splitting field for $a(x, y)$. Therefore Λ is a splitting field for each factor $a_i(x, y)$ over Ω. Thus either each $a_i(x, y)$ is absolutely irreducible in which case Ω contains $\Sigma_K(a)$ and the Lemma holds, or some $a_i(x, y)$, say for $i = 1$, factors further in $\Lambda[x, y]$.

Let

$$a_1(x, y) = a_{11}(x, y) \ldots a_{1s}(x, y)$$

where each $a_{1j}(x, y)$ is irreducible in $\Lambda[x, y]$ and monic in x. We now show that the assumption $s > 1$ leads to a contradiction.

Note that since Λ contains $\Sigma_\Omega(a_1)$ and since $a_1(x, y)$ is monic in x, it follows that each $a_{1j}(x, y)$ is a polynomial of $\Sigma_\Omega(a_1)[x, y]$. Therefore by Lemma B, each $a_{1i}(x, y)$ can be carried onto each $a_{1j}(x, y)$ by some automorphism of $\Sigma_\Omega(a_1)$ over Ω, which may be extended to an automorphism of Λ over Ω. Arrange each of the polynomials $a_1(x, y)$, $a_{11}(x, y)$, $a_{12}(x, y), \ldots, a_{1s}(x, y)$ into a sum of homogeneous terms and let $P(x, y)$, $Q_1(x, y), Q_2(x, y), \ldots, Q_s(x, y)$ be the terms of largest homogeneous degree respectively. Then because the $a_{1j}(x, y)$ are conjugate over Ω, it follows that the $Q_i(x, y)$ are conjugate over Ω. Moreover,

$$P(x, y) = \prod_{i=1}^{s} Q_i(x, y).$$

Hence

$$P(x, a) = \prod_{i=1}^{s} Q_i(x, a).$$

But $P(x, y)$ divides $F(x, y)$ and thus $P(x, a)$ divides $F(x, a)$. However the $Q_i(x, a)$ are conjugate over Ω and are at the same time in $\Omega[x]$ since $Q_i(x, a)$ is the product of factors of the form $x-\theta$ where θ is a root of $g(x) = F(x, a) = 0$. This is of course an absurdity since $F(x, a)$ and hence $P(x, a)$ has no double roots. Therefore $s = 1$ and $\Lambda = \Omega$. This proves the Lemma.

Remark. Under the conditions of Lemma C, we see that if $F(x, a)$ has no double roots for some a in K, then $\Sigma_K(a)$ is a separable extension of K.

Remark. Lemma C seems to explain why a regular polynomial chosen at random is usually absolutely irreducible. For instance, over the field Q of rational numbers, let $a(x, y)$ in $Q[x, y]$ be regular in x and of the form

$$a(x, y) = F(x, y) + (\text{lower degree terms})$$

where $F(x, y)$ is homogeneous and has no repeated factors. Choose a in K such that $F(x, a)$ has no repeated roots. Let Ω be the splitting field of the polynomial $g(x) = F(x, a)$ over Q. Then Lemma C gives us that $\Sigma_K(a)$ is a subfield of Ω. On the other hand, by the Hilbert Irreducibility Theorem, for a set of integers c of density 1, $a(x, y)-c$ is irreducible over Ω and hence absolutely irreducible. That is to say, for almost every rational perturbation of the constant term of $a(x, y)$, the resulting polynomial will be absolutely irreducible.

Definition 3. If $f(x)$ in $K[x]$ is of the form $f(x) = x^n - a$, then $f(x)$ is said to be a *pure* polynomial.

Lemma D. *Let p be a prime natural number and let a be an element of K. Then the pure polynomial $x^p - a$ is either irreducible over K or has a linear factor in $K[x]$.*

Proof. See [2], page 171.

Lemma E. *Let m be an odd natural number such that $\operatorname{char} K \nmid m$, and let a be an element of K. Then the pure polynomial $x^m - a$ is either irreducible over K or has a pure factor $x^d - b$ in $K[x]$ where $d \mid m$ and $d < m$.*

Proof (1). We proceed by induction on m. The conclusion holds for $m =$ prime by Lemma D. Assume that the Lemma holds for all allowable degrees less than m where m is an odd natural number such that $\operatorname{char} K \nmid m$. Assume that $x^m - a$ factors in $K[x]$. Hence every root of $x^m - a = 0$ has degree less than m over K. Let p be a prime divisor of m and put $k = m/p$. If $x^k - a$ reduces in $K[x]$, then by induction, $x^m - a$ has a factor in $K[x]$ of the required form. Therefore assume that $x^k - a$ is irreducible over K.

Let β be a root of $x^k - a = 0$. Consider the polynomial $x^p - \beta$. By Lemma D, either $x^p - \beta$ is irreducible over $K(\beta)$ or has a linear factor in $K(\beta)[x]$. The first case cannot occur for if $x^p - \beta$ were irreducible over $K(\beta)$ and if α were a root, then α would be a root of $x^m - a = 0$ of degree m over K, thus contradicting the reducibility of $x^m - a$ in $K[x]$. Therefore $x^p - \beta = 0$ has a root α in $K(\beta)$. Hence $\alpha^p = \beta$.

Let $N(\gamma)$ denote the norm of an element γ in $K(\beta)$ over K. Then

$$N(\beta) = (-1)^k(-a) = N(\alpha^p) = N(\alpha)^p = a$$

since m is odd. Therefore a is a pth power in K and so $x^m - a$ has the factor $x^k - N(\alpha)$ in $K[x]$. This completes the proof of Lemma E.

Remark. The assumption that m be odd in Lemma E is necessary as can be seen by the example in $Z_3[x]$ of

$$x^4 - 2 = (x^2 + x - 1)(x^2 - x - 1).$$

(1) The author wishes to thank H. B. Mann for his suggestions concerning the proofs of this and the following Lemma.

Lemma F. *Suppose that the pure polynomial x^n-a is irreducible in $K[x]$ and that* $\operatorname{char} K \nmid n$. *Let a be a root of $x^n-a=0$. If K contains no n-th roots of unity other than* 1, *then there are no proper extensions Ω normal over K such that*

$$K \subset \Omega \subset K(a).$$

Proof. Suppose contrary to what is to be proved that Ω is a proper normal extension of K that is contained in $K(a)$. We may assume that Ω is a maximal such extension of K. Let $d = (K(a):\Omega)$, i.e., the degree of $K(a)$ over Ω. Then $d|n$. Let the conjugates of a over Ω be $a = a_1, \ldots, a_d$. Let $\beta = a_1 \ldots a_d$. Then β is an element of Ω and is of the form $\beta = a^d\zeta$ where ζ is an nth root of unity. Note that $\zeta = \beta/a^d$ is in $K(a)$ and therefore is in Ω since $\Omega(\zeta)$ is a normal extension of K contained in $K(a)$ while Ω is a maximal such extension. Therefore $\gamma = \beta/\zeta = a^d$ is in Ω.

Note that x^m-a is irreducible over K for any divisor m of n and in particular for $m = n/d$. But $x^m-a = 0$ has γ as a root and hence $\Omega = K(\gamma)$ since $m = (K(\gamma):K) = (\Omega:K)$. Since Ω is normal over K, it must contain the conjugates of γ and hence contains a primitive mth root of unity. Let p be the smallest prime divisor of m. Let $\mathscr{E}$ be a primitive pth root of unity. Then $\mathscr{E}$ is an element of Ω since pth roots of unity are mth roots of unity. But then $(K(\mathscr{E}):K)|p-1$ and $(K(\mathscr{E}):K)|m$. Since p was chosen as the smallest prime divisor of m, these divisor relations are contradictory unless $(K(\mathscr{E}):K) = 1$. Hence K contains an nth root of unity other than 1, contrary to our assumptions. This proves Lemma F.

Lemma G. *Suppose that* $\operatorname{char} K \nmid m$, *that a is an element of K, and that K contains no m-th roots of unity other than* 1. *Then there is a root a of $x^m-a=0$ such that for each root of unity ζ in the algebraic closure A of K,*

$$K(a) \cap K(\zeta) = K.$$

Proof. Note that because $\operatorname{char} K \nmid m$ and since K contains no nth roots of unity other than 1, we may conclude that m is odd.

Let d be the minimum divisor of m such that x^m-a has a pure factor x^d-b in $K[x]$. Then by Lemma E, x^d-b is irreducible in $K[x]$. Let a be a root of $x^d-b=0$. Clearly K contains no dth roots of unity other than 1 since dth roots are mth roots of unity. It follows by Lemma F that no subfield of $K(a)$ is normal over K except K itself. Let ζ be a root of unity in A. Then $K(\zeta)$ is a normal separable abelian extension of K. Therefore the field

$$\Omega = K(a) \cap K(\zeta)$$

is normal over K since it is a subfield of an abelian extension. Therefore $\Omega = K$ and the Lemma is proven.

Remark. Actually we may conclude that there is a root a of $x^m-a=0$ such that $K(a)$ meets every abelian extension only at K itself.

We now direct our attention to polynomials exceptional over K.

Lemma H. *Suppose $f(x)$ is exceptional over K and yet $f(a) = f(b)$ for some $a \neq b$ in K. Then $f'(a) = f'(b) = 0$.*

Proof. Let $\Phi(x,y) = (f(x)-f(y))/(x-y)$. Then $\Phi(a,b) = 0$. But $\Phi(x,y)$ is within a constant of K the product of polynomials monic in x and irreducible in $K[x,y]$, each of which is the product of two or more conjugate polynomials in $\Sigma_K(\Phi)[x,y]$. Therefore since the point (a,b) has coordinates drawn from K, it is at least a double point of the curve $\Phi(x,y)=0$. Therefore (a,b) is at least a double point of the curve $F(x,y) = f(x)-f(y) = 0$ and so

$$\frac{\partial F(a,b)}{\partial x} = f'(a) = \frac{\partial F(a,b)}{\partial y} = -f'(b) = 0.$$

Lemma I. *Suppose $f(x)$ in $K[x]$ is of the form*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_r x^r$$

where $r > 1$ and $\operatorname{char} K \nmid r$. *If $f(x)$ is exceptional over K, then K contains no r-th roots of unity other than* 1.

Proof. Suppose that $f(x)$ is exceptional over K. Let

$$\Phi(x,y) = a_n \Phi_1(x,y) \ldots \Phi_s(x,y)$$

where each $\Phi_i(x,y)$ is irreducible in $K[x,y]$ and monic in x. Arrange each $\Phi_i(x,y)$ into a sum of homogeneous terms and let $P_i(x,y)$ be the term of least homogeneous degree in $\Phi_i(x,y)$. Then

$$a_r E_r(x,y) = a_n \prod_{i=1}^{s} P_i(x,y)$$

where

$$E_r(x,y) = (x^r-y^r)/(x-y) = \prod_{\substack{\zeta^r=1\\ \zeta\neq 1}} (x-\zeta y).$$

Suppose ζ is a rth root of unity in K other than 1. Then $x-\zeta y$ is a factor of $E_r(x,y)$ and hence divides some $P_i(x,y)$, say for $i=1$. But by Lemma B, $\Phi_1(x,y)$ is the product of k conjugate irreducible polynomials $\Phi_{11}(x,y), \ldots, \Phi_{1k}(x,y)$ in $\Sigma_K(\Phi)[x,y]$ that are monic in x. Since $f(x)$ is exceptional over K, $k > 1$. Arrange each $\Phi_{1i}(x,y)$ into a sum of homogeneous terms and let $Q_i(x,y)$ denote the term of least homogeneous degree in $\Phi_{1i}(x, y)$. Then

$$P_1(x, y) = \prod_{i=1}^{k} Q_i(x, y).$$

Moreover, since the $\Phi_{1i}(x, y)$ are conjugate over K, so are the $Q_i(x, y)$. On the other hand, $x-\zeta y$ divides $P_1(x, y)$ and hence divides some $Q_i(x, y)$; therefore $x-\zeta y$ divides each $Q_i(x, y)$ since ζ is in K. This is an absurdity since $E_r(x, y)$ and hence $P_1(x, y)$ has no repeated factors when $\operatorname{char} K \nmid r$. This proves the Lemma.

Remark. Suppose $(\operatorname{char} K, 2n) = 1$. If $f(x)$ is exceptional over K of degree n, then n is odd. For if we apply the methods of the above proof to the homogeneous terms of largest degree, we see that K cannot contain nth roots of unity other than 1. Hence n must be odd.

LEMMA J. *Suppose that $f(x)$ in $K[x]$ is exceptional over K and is of degree n where $\operatorname{char} K \nmid n$. Let ζ be a primitive n-th root of unity over K. Suppose that Ω is a finite extension of K such that*

$$\Omega \cap K(\zeta) = K.$$

Then $f(x)$ is exceptional over Ω.

Proof. Let $\Phi(x, y) = \big(f(x)-f(y)\big)/(x-y)$. If $f(x)$ is no longer exceptional over Ω, then $\Phi(x, y)$ has an absolutely irreducible factor $\Phi_1(x, y)$ in $\Omega[x, y]$ that we may assume is monic in x. Hence $\Phi_1(x, y)$ must coincide with an irreducible factor of $\Phi(x, y)$ in $\Sigma_K(\Phi)[x, y]$ that is monic in x. But by Lemma C, $\Sigma_K(\Phi)$ is a subfield of $K(\zeta)$ since the homogeneous term of $\Phi(x, y)$ of largest degree is, within a constant of K, $E_n(x, y) = (x^n-y^n)/(x-y)$. Hence the coefficients of $\Phi_1(x, y)$ are elements of $K(\zeta)$. On the other hand, $\Omega \cap K(\zeta) = K$ which implies that $\Phi_1(x, y)$ is in $K[x, y]$, contradicting exceptionality. This proves the Lemma.

We are now finally in a position to prove Theorem 1:

Proof of Theorem 1. Suppose $f(x)$ in $K[x]$ is exceptional over K of degree n where $\operatorname{char} K = 0$ or $n < \operatorname{char} K$. Let A be the algebraic closure of K. Then by Zorn's Lemma there is a maximal subfield Ω of A such that $f(x)$ is exceptional over Ω. If $f(x)$ is a one-to-one map of Ω into Ω, then $f(x)$ is a fortiori univalent on K. Therefore for our purposes, it is sufficient to assume that $K = \Omega$, i.e., that $f(x)$ is exceptional over K but not exceptional over any finite extension of K.

Suppose that $f(x)$ is not univalent on K. Then $f(a) = f(b)$ for some $a \neq b$ in K. We may assume that $a = 0$, $b = 1$, and $f(0) = f(1) = 0$ since $f(x)$ is simultaneously exceptional and/or univalent with the polynomial $\alpha f(\beta x+\gamma)+\delta$ when $\alpha\beta \neq 0$.

Let

$$f(x) = a_n x^n + \ldots + a_r x^r$$

and

$$f(x+1) = b_n x^n + \ldots + b_s x^s;$$

we may assume that $b_s = 1$.

Then by Lemma H, $r > 1$ and $s > 1$. Since $\operatorname{char} K = 0$ or $n < \operatorname{char} K$, we see that $\operatorname{char} K \nmid rs$. Then by Lemma I, K contains no rth nor sth roots of unity other than 1. Let ζ be a primitive nth root of unity over K. Then by Lemma G, there is a root α of the equation $x^r - a_r = 0$ such that

$$K(\alpha) \cap K(\zeta) = K.$$

Hence by Lemma J, $f(x)$ is exceptional over $K(\alpha)$. Therefore $K(\alpha) = K$ by the maximality assumption on K. Hence α is already in K. Likewise there is a root β of the equation $x^s - \alpha = 0$ in K. Therefore $x^{rs} - a_r = 0$ has a root β in K.

Let $\Phi(x, y) = \big(f(x)-f(y)\big)/(x-y)$. Then

$$f(x^s) - f(y^r+1) = (x^s - y^r - 1)\,\Phi(x^s, y^r+1).$$

Therefore equating the homogeneous terms of least degree, we have

$$a_r x^{rs} - y^{rs} = -P(x, y)$$

where $P(x, y)$ is the homogeneous term of $\Phi(x^s, y^r+1)$ of least degree. Hence

$$x^{rs} - 1 = -P(x/\beta, 1).$$

Let $Q(x) = -P(x/\beta, 1)$. Note that 1 is a simple root of $Q(x)$ since $\operatorname{char} K \nmid rs$. On the other hand, $\Phi(x, y)$ is within a constant of K the product of irreducible factors $\Phi_1(x, y), \ldots, \Phi_k(x, y)$ in $K[x, y]$ that are monic in x. Because $f(x)$ is exceptional, each $\Phi_i(x, y)$ is the product of two or more conjugate factors in $\Sigma_K(\Phi)[x, y]$. Therefore in turn, $P(x, y)$ is within a constant of K the product of polynomials in $K[x, y]$, each of which is the product of two or more conjugate polynomials in $\Sigma_K(\Phi)[x, y]$. Therefore $Q(x)$ is within a constant of K the product of polynomials in $K[x]$, each of which is the product of conjugate polynomials in $\Sigma_K(\Phi)[x]$. Therefore every root of $Q(x)$ in K is a repeated root. This contradicts the above conclusion that 1 is a simple root of $Q(x)$. This proves Theorem 1.

Remark. Theorem 1 together with what was shown by Davenport and Lewis in [1] shows that for $f(x)$ in $Z[x]$ and for all large primes, $f(x)$ is exceptional modulo p if and only if $f(x)$ permutes the residue classes modulo p, i.e., the exceptional polynomials coincide with the one-to-one polynomials.

2. Exceptional polynomials over finite fields. The first proof that was obtained for the Davenport-Lewis Conjecture applied to finite fields and is interesting enough to be presented here in outline:

Let K be the finite field of characteristic p and order p^d. Let Γ be the complete valuation field of all formal power series in the transcendental u with coefficients drawn from K. If $f(x)$ is exceptional over K, then $f(x)$ is exceptional over Γ. For any polynomial $f(x)$ in $K[x]$, if $f(a) = f(b)$ for some $a \neq b$ in K, and if a has order r as a root of $f(x)-f(a)$ where $(r, p(p^d-1)) = 1$, then by a form of Hensel's Lemma it follows that the set

$$R = \{z \text{ in } \Gamma;\ f(z) = f(w) \text{ for some } w \neq z \text{ in } \Gamma\}$$

is infinite. If $f(x)$ is in addition exceptional over K, then the condition $(r, p^d-1) = 1$ is a Corollary of Lemma I provided that $(r, p) = 1$. On the other hand, if $f(x)$ is exceptional over K, then R must be an finite set by Lemma H. From all this we obtain

THEOREM 2. *If $f(x)$ is exceptional over the finite field K of characteristic p and if the degree of $f(x)$ is n where $n < 2p$, then $f(x)$ is a one-to-one map of K onto K.*

3. The case $n \geqslant \operatorname{char} K$. It is at this time an open question whether exceptional polynomials are univalent without qualification. The author and others have been unable to find a single polynomial that is exceptional over a field that is not univalent on the given field. There are compelling reasons to believe that no such examples exist. For example, if $f(x)$ is exceptional over K, and in addition, if $\Phi(x, y) = (f(x)-f(y))/(x-y)$ is irreducible in $K[x, y]$, then it follows that $f(x)$ is univalent on K; for if s is the number of conjugate factors of $\Phi(x, y)$ in $\Sigma_K(\Phi)[x, y]$, then by comparing the order of the factor $x-a$ in the polynomial

$$f(x)-f(a) = (x-a)\Phi(x, a) = (x-b)\Phi(x, b),$$

we are led to an equation of the form $1+ks = ms$ when $f(a) = f(b)$ for some $a \neq b$ in K.

The author has computed several cases not covered by Theorems 1 and 2 and has found that every polynomial $f(x)$ of degree $n = 3, 4, 5, \ldots, 13$ that is exceptional over Z_p for $p = 2, 3, 5, 7, 11, 13$, is necessarily univalent on Z_p. For these and other reasons, the author

feels that if there are exceptional polynomials that are not univalent, then they must occur over imperfect fields.

I wish to thank Professor D. J. Lewis for initially suggesting this problem and for his valuable assistance. I would also like to thank Professor H. Davenport for an observation which led to a simplification of the original proof of Theorem 1.

References

[1] H. Davenport and D. J. Lewis, *Notes on Congruences I*, Quart. J. Math. Oxford (2), 14 (1963), pp. 51-60.

[2] B. L. van der Waerden, *Modern Algebra*, New York 1948.

Reçu par la Rédaction le 8. 6. 1966