LINEAR DIVISIBILITY SEQUENCES*

BY

MORGAN WARD

I. Introduction

1. A sequence of rational integers

$$(u): \qquad u_0, u_1, \cdots, u_n, \cdots$$

is called a *divisibility sequence* if u_n divides u_m whenever n divides m. (u) is *linear*† if it satisfies a linear difference equation with integral coefficients and *normal* if $u_0 = 0$, $u_1 = 1$. Marshall Hall has shown that a linear divisibility sequence is usually normal [2]. If

$$(1.1) \qquad f(x) = x^k - c_1 x^{k-1} - \cdots - c_k, \qquad c_1, \cdots, c_k \text{ integers},$$

is the polynomial associated with the difference equation of lowest order which (u) satisfies, (u) is said to be of *order* k and to *belong to* its *characteristic polynomial* $f(x)$.

An integer dividing every term of (u) beyond a certain point is called a *null divisor* of (u) [3]. If (u) has no null divisors save ± 1, it is said to be *primary*.

If u_s is any fixed non-vanishing term of (u), the sequence

$$u_0/u_s, u_s/u_s, u_{2s}/u_s, \cdots, u_{ns}/u_s, \cdots$$

is called a *subsequence* of (u). The various subsequences of (u) are themselves normal linear divisibility sequences of order $\leqq k$.

2. The object of this paper is to prove the following results:

Let the characteristic polynomial of the linear divisibility sequence (u) have no repeated roots, and let its coefficients be relatively prime. Then:

I. *If (u) is primary and if q is any large prime number,*

$$(2.1) \qquad u_q^\sigma \equiv 1 \pmod{q},$$

where σ is the least common multiple of 1, 2, 3, $\cdots$, k.

II. *If (u) is not primary it always contains an infinity of subsequences which are primary. Furthermore the characteristic polynomials of such subsequences satisfy the hypotheses imposed above upon the polynomial* (1.1).

* Presented to the Society, June 18, 1936; received by the editors May 5, 1936.

† T. A. Pierce appears to have been the first to discuss sequences of order greater than two [1]. (Numbers in square brackets refer to the bibliography at the end of the paper.)

III. *There exists a rational number*

$$B = B(u) = B(u_0, u_1, \cdots, u_{k-1}; c_1, \cdots, c_k) = \frac{P}{Q}, \qquad (P, Q) = 1$$

such that

(i) *if p is a prime number dividing neither the numerator P nor the denominator Q of B, then the rank of apparition* of p in the sequence (u) is the restricted period* of (u) modulo p;*

(ii) *the prime factors of the denominator of B all divide the discriminant of the polynomial to which (u) belongs;*

(iii) *the numerator of B can never vanish if the galois group of $f(x)$ is alternating or symmetric.*†

II. Proof of first result

3. Given any modulus m, the least period of (u) modulo m is called its characteristic number and the number of non-periodic terms in (u) modulo m its numeric. The reader will be assumed to be familiar with my previous paper in these Transactions [4] (referred to hereafter as T) devoted to the determination of these numbers.

Henceforth let (u) be a normal linear divisibility sequence of order k, and let D denote the discriminant of its characteristic polynomial. We assume:

$$D \neq 0. \tag{3.1}$$

Lemma 3.1 [4]. *If‡ $(q, D)=1$, q a prime, and if σ is the least common multiple of 2, 3, $\cdots$, k, then (u) admits the period $q^\sigma - 1$ modulo q.*

Theorem 3.1. *If (u) is a linear divisibility sequence of order k and q a prime such that $u_q \equiv 0 \pmod q$, then either q divides D or q divides c_k.*

Assume that‡ $q \mid u_q$, q a prime. The assumption $(q, c_k) = (q, D) = 1$ then yields a contradiction. For if $(q, c_k)=1$, (u) is purely periodic modulo q [5]. And if $(q, D)=1$, (u) admits the period $q^\sigma - 1$ modulo q. Determine positive integers x and y such that $xq = y\,(q^\sigma - 1) + 1$. Then $u_{xq} \equiv u_1 \equiv 1 \pmod q$. But $q \mid u_q$ and $u_q \mid u_{xq}$.

The following lemma is a direct consequence of Theorem 3.1.

* The rank of apparition of p is the index ρ of the first term of (u) excluding u_0 which divides: $u_\tau \equiv 0 \pmod p$; $u_n \not\equiv 0 \pmod p$, $0 < n < \rho$. The restricted period [5] of (u) modulo is the least positive integer τ such that $u_{n+\tau} \equiv c u_n \pmod p$, $n = 0, 1, 2, \cdots$, c an integer. ρ always divides τ [2].

† It is unknown whether divisibility sequences exist whose characteristic polynomial is restricted as in (iii). No such sequences exist when $k=3$ [2].

‡ If $a, b, c, \cdots$ are rational integers, we write as usual $(a, b, c, \cdots)$ for the greatest common divisor of $a, b, c, \cdots$, and $a \mid b$ for a divides b.

LEMMA 3.2. *There exists a rational integer* q_0 *such that*

$$u_q \not\equiv 0 \pmod{q}, \qquad q \text{ a prime} \geqq q_0. \tag{3.2}$$

LEMMA 3.3 [4]. *For any prime* p, $p^k(p^\sigma - 1)$ *is a period of* (u) *modulo* p.

LEMMA 3.4 [4]. *For any prime* p, *the numeric of* (u) *modulo* p *is less than or equal to* k.

THEOREM 3.2. *If* p *is a prime dividing a term* u_q *of the divisibility sequence* (u) *with a sufficiently large prime index* q, *then either*

$$p^\sigma \equiv 1 \pmod{q} \tag{3.3}$$

or else (u) *is a null sequence modulo* p.

Choose a prime $q > k$ and q_0 of (3.2), and assume that $u_q \equiv 0 \pmod{p}$, p a prime. By (3.2), $p \neq q$. Hence if $(p^\sigma - 1, q) = 1$, for each positive integer r there exist positive integers x, y, z such that

$$xq + yp^k(p^\sigma - 1) = r + zp^k(p^\sigma - 1). \tag{3.4}$$

By Lemma 3.3, $p^k(p^\sigma - 1)$ is a period of (u) modulo p. Therefore if $r > k$, (3.4) and Lemma 3.4 give $u_{xq} \equiv u_r \pmod{p}$. Since $p \mid u_q$ and $u_q \mid u_{xq}$, $u_r \equiv 0 \pmod{p}$ so that (u) is a null sequence modulo p.

THEOREM 3.3. *If the linear divisibility sequence* (u) *is primary, and if* k *is its order and* σ *the least common multiple of the numbers* $2, 3, \cdots, k$, *then for all sufficiently large prime indices* q *we have*

$$u_q^\sigma \equiv 1 \pmod{q}. \tag{2.1}$$

Choose the prime $q > k$ and q_0 of (3.2), and let the factorization of u_q be $u_q = p_1^{s_1} p_2^{s_2} \cdots p_t^{s_t}$. Since (u) is assumed primary none of the primes p_i are null divisors. Therefore Theorem 3.2, $p_i^\sigma \equiv 1 \pmod{q}$, so that

$$p_i^{\sigma s_i} \equiv 1 \pmod{q}, \qquad (i = 1, 2, \cdots, t).$$

On multiplying these t congruences together, we obtain (2.1), and our first result is proved.

III. PROOF OF SECOND RESULT

4. We assume that (u) is a normal linear divisibility sequence for which

$$(c_1, c_2, \cdots, c_k) = 1. \tag{4.1}$$

A *proper* null divisor of a linear sequence is one which divides neither its initial terms nor the coefficients of its recursion. Any other null divisor is called *trivial*. (u) obviously has no trivial null divisors.

THEOREM 4.1. *No subsequence of (u) has trivial null divisors.*

LEMMA 4.1 (Schatanovskis Principle) [6, 7, 8]. *If $\Phi(x_1, x_2, \cdots, x_k)$ is an integral symmetric function of the arguments $x_1, \cdots, x_k$ with integral coefficients, and if for a natural number m*

$$f(x) \equiv (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k) \equiv (x - \gamma_1)(x - \gamma_2) \cdots (x - \gamma_k) \pmod{m},$$

where $f(x)$ is a polynomial with integral coefficients, then

$$\Phi(\alpha_1, \alpha_2, \cdots, \alpha_k) \equiv \Phi(\gamma_1, \gamma_2, \cdots, \gamma_k) \pmod{m}.$$

LEMMA 4.2. *Let*

$$f^{(s)}(x) = x^k - d_1x^{k-1} - \cdots - d_k$$

be the polynomial whose roots are the sth powers of the roots of $f(x)$, and p a prime number. Then if t is any positive integer $\leqq k$, (A) $p \mid (c_k, c_{k-1}, \cdots, c_{k-t+1})$ *when and only when* (B) $p \mid (d_k, d_{k-1}, \cdots, d_{k-t+1})$.

Assume that (A) holds. Then

$$f(x) \equiv g(x) = x^{k-t}(x^t - c_1x^{t-1} - \cdots - c_{k-t}) \pmod{p}.$$

Let the k roots of $g(x) = 0$ be $\gamma_1, \gamma_2, \cdots, \gamma_t$; $\gamma_{t+1} = \gamma_{t+2} = \cdots = \gamma_k = 0$. If the roots of $f(x) = 0$ are $\alpha_1, \alpha_2, \cdots, \alpha_k$, then $d_i = \Phi(\alpha_1, \alpha_2, \cdots, \alpha_k)$, where Φ is a symmetric polynomial in its arguments with rational integral coefficients. Hence by the preceding lemma

$$d_i \equiv \Phi(\gamma_1, \gamma_2, \cdots, \gamma_k) \pmod{p}.$$

But if $g^{(s)}(x) = x^k - e_1x^{k-1} - \cdots - e_k$ is the equation whose roots are the sth powers of the roots of $g(x) = 0$, then

$$e_i = \Phi(\gamma_1, \gamma_2, \cdots, \gamma_k) = \Sigma\gamma_1^s\gamma_2^s \cdots \gamma_i^s = 0 \text{ if } i > k - t.$$

Hence $d_i \equiv 0 \pmod{p}$ if $i > k - t$, so that (B) follows.

To prove the converse, it suffices to show that (A) and $c_{k-t} \not\equiv 0 \pmod{p}$ imply that $d_{k-t} \not\equiv 0 \pmod{p}$. But by what precedes,

$$d_{k-t} \equiv \Sigma(\gamma_1\gamma_2 \cdots \gamma_t)^s \equiv (\gamma_1\gamma_2 \cdots \gamma_t)^s \equiv c_{k-t}^s \pmod{p}.$$

Proof of Theorem 4.1. With the notation of Lemma 4.2, any subsequence (v): $v_n = u_{ns}/u_s$ of (u) is normal, so that the only possible trivial null divisors of (v) are common divisors of $d_1, d_2, \cdots, d_k$. On taking $t = k$ in Lemma 4.2, we see that if $(c_1, c_2, \cdots, c_k) = 1$ then $(d_1, d_2, \cdots, d_k) = 1$.

5. We begin our discussion of the proper null divisors of (u) by restating some properties of linear sequences used in T. Let

$$f_0(x) = 0, \; f_r(x) = x^r - c_1x^{r-1} - \cdots - c_r, \qquad (r = 1, 2, \cdots, k).$$

The polynomial

$$u(x) = u_0 f_{k-1}(x) + u_1 f_{k-2}(x) + \cdots + u_{k-1} f_0(x) \tag{5.1}$$

is called the *generator* of the sequence (u).* If furthermore

$$\Delta(u) = \begin{vmatrix} u_0, & u_1, \cdots, & u_{k-1} \\ u_1, & u_2, \cdots, & u_k \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ u_{k-1}, & u_k, \cdots, & u_{2k-2} \end{vmatrix}, \tag{5.2}$$

then

$$\Delta(u) = (-1)^{k(k-1)/2} \operatorname{Res}\{u(x), f(x)\} = \beta_1\beta_2 \cdots \beta_k D, \tag{5.3}$$

where $u_n = \beta_1\alpha_1^n + \cdots + \beta_k\alpha_k^n$ and $\alpha_1, \cdots, \alpha_k$ are the roots of $f(x)$. Since (u) is of order k and $D \neq 0$, $\Delta(u) \neq 0$.

Consider next the $k+1$ greatest common divisors

$$\begin{aligned} e_0 &= (u_0, u_1, u_2, \quad \cdots, u_{k-1}) \\ e_1 &= (c_k, u_1, u_2, \quad \cdots, u_{k-1}) \\ e_2 &= (c_k, c_{k-1}, u_2, \quad \cdots, u_{k-1}) \\ &\cdots\cdots\cdots\cdots \\ e_{k-1} &= (c_k, c_{k-1}, c_{k-2}, \cdots, u_{k-1}) \\ e_k &= (c_k, c_{k-1}, c_{k-2}, \cdots, c_1). \end{aligned}$$

Then

$$e_0 = e_1 = e_k = 1.$$

The following lemma easily follows from formula (5.1) and the results of part IV of T.

LEMMA 5.1. *Necessary and sufficient conditions that a linear sequence of order k be primary are that the $k+1$ greatest common divisors e_i be all equal to unity.*

THEOREM 5.1. *If the prime p is a null divisor of the normal linear divisibility sequence (u), then p divides both $\Delta(u)$ and the discriminant D of the characteristic polynomial $f(x)$ of (u).*

It is easily shown that every such p must divide one or the other of the numbers e_i. Since $e_k = 1$, $p \mid u_{k-1}$. Hence $p \mid u_k$, $p \mid u_{k+1}, \cdots$ by Lemma 3.4.

* We have the identity $u(x)/f(x) = \sum_0^\alpha u_n/x^{n+1}$ for $|x|$ large. See T, p. 606, and [3].

Hence $p|\Delta(u)$ by formula (5.2). Since $e_0=e_1=1$, $p|c_k$ and $p|c_{k-1}$. Hence $x=0$ is a multiple root of the congruence $f(x)\equiv 0 \pmod{p}$ and $p|D$.

As a corollary, we have

LEMMA 5.2. *A sufficient condition that the divisibility sequence* (u) *be primary is that* D *and* $\Delta(u)$ *be co-prime.*

If p is a prime proper null divisor of (u), the exponent of the highest power of p which is a null divisor of (u) is called the *index* of p in (u) [3].

LEMMA 5.3 [3]. *Let* (u) *be a linear sequence for which* (4.1) *holds. Then the index of any prime null divisor* p *is* $\leqq r$, *where* p^r *is the highest power of* p *dividing* $\Delta(u)$.

THEOREM 5.2. *A subsequence of a normal linear divisibility sequence can have no prime null divisor which is not a possible null divisor of* (u) *itself.*

Every prime null divisor of (u) must divide c_k in (1.1) [5]. Let (v) be any subsequence of (u). By Theorem 4.1, (v) can have only proper null divisors. Hence any prime null divisor of (v) must divide the constant term d_k of the polynomial to which (v) belongs. But obviously d_k divides some power of c_k.

6. Let $f^{(s)}(x)=(x-\alpha_1^s)\cdots(x-\alpha_k^s)$ be the polynomial whose roots are the sth powers of the roots of $f(x)$, and let $D^{(s)}$ be its discriminant. $D^{(s)}/D$ is clearly an integer.

THEOREM 6.1. *The integer* s *may be chosen in an infinite number of ways so that* $D^{(s)}/D$ *is prime to* D.

Let p be any prime factor of D, $\mathfrak{F}$ the Galois field of $f(x)$, and $\mathfrak{p}$ a prime ideal factor of p in $\mathfrak{F}$. Then since $D^{1/2}=\prod_{i<j}(\alpha_i-\alpha_j)$, $p|D$ only when $\alpha_i-\alpha_j\equiv 0 \pmod{\mathfrak{p}}$ for some values of the subscripts i and j.

Now

$$\left(\frac{D^{(s)}}{D}\right)^{1/2}=\prod_{i<j}\frac{\alpha_i^s-\alpha_j^s}{\alpha_i-\alpha_j} \quad \text{and} \quad \frac{\alpha_i^s-\alpha_j^s}{\alpha_i-\alpha_j}\equiv s \pmod{[\alpha_i-\alpha_j]}.*$$

Hence if $\alpha_i-\alpha_j\equiv 0 \pmod{\mathfrak{p}}$, then $\alpha_i^s-\alpha_j^s/(\alpha_i-\alpha_j)\equiv 0 \pmod{\mathfrak{p}}$ if and only if $s\equiv 0 \pmod{\mathfrak{p}}$; that is, if and only if $s\equiv 0 \pmod{p}$. Choose s prime to D. Then if $D^{(s)}/D$ and D have a common factor, and hence a common prime factor p, we must have for some k and l

$$\text{(6.1)} \qquad \alpha_k^s \equiv \alpha_l^s \pmod{\mathfrak{p}}, \qquad\qquad \text{(6.11)} \qquad \alpha_k \not\equiv \alpha_l \pmod{\mathfrak{p}},$$

where $\mathfrak{p}|p$. If both (6.1) and (6.11) hold, then

* The square bracket denotes a principal ideal.

$$(6.2) \qquad (\alpha_k, \mathfrak{p}) = (\alpha_l, \mathfrak{p}) = (\alpha_k - \alpha_l, \mathfrak{p}) = \mathfrak{o},$$

where $\mathfrak{o}$ as usual is the unit ideal of $\mathfrak{F}$.

Now for each pair of distinct roots α_i, α_j of $f(x)$ for which $(\alpha_i, \mathfrak{p}) = (\alpha_j, \mathfrak{p}) = (\alpha_i - \alpha_j, \mathfrak{p}) = \mathfrak{o}$, let s_{ij} be the least positive integer y such that

$$(6.3) \qquad \alpha_i^y \equiv \alpha_j^y \pmod{\mathfrak{p}}.$$

Then s_{ij} divides every other such y, and in particular the number $N(\mathfrak{p}) - 1 = p^t - 1$. Here $t \leqq k!$, the maximum possible degree of $\mathfrak{F}$.

Let m_p be the least common multiple of the numbers $p-1, p^2-1, \cdots, p^{k!}-1$ and if D has in all k distinct prime factors $p_1, p_2, \cdots, p_k$ let M be the least common multiple of $m_{p_1}, m_{p_2}, \cdots, m_{p_k}$. Then if *$s$ is chosen prime to both M and D* (and this choice can be made in an infinity of ways), *$D^{(s)}/D$ is prime to D.*

For if $(s, D) = 1$ and $(D^{(s)}/D, D) \neq 1$, (6.1) holds. Then $s_{kl} | s$. Since $(s, M) = 1$ and $s_{kl} | M$, $s_{kl} = 1$ contradicting (6.11).

7. As in §6, let $p_1, \cdots, p_k$ be the distinct prime factors of D. By Theorems 4.5, 5.1 and Lemma 5.4, these primes are the only possible prime null divisors of (u) and its subsequences. Write

$$\Delta(u) = p_1^{r_1} \cdots p_k^{r_k} q, \qquad (q, D) = 1, \qquad r_i \geqq 0,$$

and let θ_i be the index of p_i in (u), where if p_i is not a null divisor, $\theta_i = 0$. By Lemma 5.3, $0 \leqq \theta_i \leqq r_i$, $(i = 1, 2, \cdots, k)$.

Now if R is the largest of $r_1, r_2, \cdots, r_k$, the numeric of p^{θ_i} is always less than kR^s. Choose $s > kR$ as in Theorem 6.1, and let (v) be the subsequence of (u) with general term $v_n = u_{ns}/u_s$ belonging to the polynomial $f^{(s)}(x)$. As in Theorem 6.1, let the discriminant of $f^{(s)}(x)$ be $D^{(s)}$. Then since $u_{ns} = \beta_1 \alpha_1^{ns} + \cdots + \beta_k \alpha_k^{ns}$, we have by formula (5.3),

$$(7.1) \qquad \Delta(v) = \frac{\Delta(u)}{u_s^k} \frac{D^{(s)}}{D}.$$

Now $u_s \equiv 0 \pmod{p_i^{\theta_i}}$ and $(p_i, D^{(s)}/D) = 1$. Hence since $\Delta(v)$ is an integer, $\Delta(u) \equiv 0 \pmod{p_i^{k\theta_i}}$. Therefore $r_i \geqq k\theta_i$. If $\Delta(v) = p_1^{r_1'} \cdots p_k^{r_k'} q'$, $(q', D) = 1$, then $r_i' = r_i - k\theta_i$. Therefore

$$(7.2) \qquad r_i' < r_i \text{ if } \theta_i > 0; \; r_i' = r_i \text{ if } \theta_i = 0.$$

8. We now prove our second result indirectly. Suppose that the result is false. Then in any infinite set of normal divisibility sequences

$$\mathfrak{S}: \quad (u^{(1)}) = (u), (u^{(2)}), (u^{(3)}), \cdots, (u^{(m)}), (u^{(m+1)}), \cdots,$$

such that each sequence is a subsequence of its immediate predecessor, there must occur an infinity of non-primary sequences. Therefore there must exist a prime p dividing D which is a null divisor of an infinite number of the sequences $(u^{(m)})$. The general term of $(u^{(m+1)})$ is of the form $u_n^{(m+1)} = u_{ns_m}^{(m)}/u_{s_m}^{(m)}$, where the integer s_m specifies the particular subsequence of $(u^{(m)})$ selected. Consider now a set $\mathfrak{S}$ in which each $u^{(m)}$ satisfies the conditions imposed upon s in §6.

The considerations of the preceding section carry over to the relationship between $(u^{(m)})$ and $(u^{(m+1)})$. With an obvious extension of notation, let $\theta^{(m)}$ denote the index of p in $(u^{(m)})$ and p^{r_m} and $p^{r_{m+1}}$ the highest powers of p dividing $\Delta(u^{(m)})$ and $\Delta(u^{(m+1)})$. Then as in (7.2)

$$r_{m+1} < r_m \text{ if } \theta^{(m)} > 0; \; r_{m+1} = r_m \text{ if } \theta^{(m)} = 0. \tag{8.1}$$

By our hypothesis, an infinite number of the $\theta^{(m)}$ are positive. But then (8.1) leads to an absurdity; for obviously $r = r_1 \geqq r_2 \geqq r_3 \geqq \cdots \geqq 0$.

IV. Proof of third result

9. We assume as in the previous proofs that $D \neq 0$. In the Galois field $\mathfrak{F}$ of $f(x)$, a rational prime p which does not divide D remains unramified [9]. Accordingly the decomposition of p into prime ideal factors in $\mathfrak{F}$ is of the form

$$p = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_l,$$

where the $\mathfrak{p}$ are all distinct.

Let σ_i be the least positive integer n such that

$$\alpha_1^n \equiv \alpha_2^n \equiv \cdots \equiv \alpha_k^n \pmod{\mathfrak{p}_i} \qquad (i = 1, \cdots, l). \tag{9.1}$$

The restricted period τ of (u) modulo p is defined as the least value of n such that

$$u_{n+m} \equiv au_n \pmod{p} \qquad (m = 0, 1, 2, \cdots),$$

where a is some rational integer [5]. If p is prime to $\Delta(u)$, τ may be equally defined as the least positive integer n such that we have in $\mathfrak{F}$

$$\alpha_1^n \equiv \alpha_2^n \equiv \cdots \equiv \alpha_k^n \pmod{p}.$$

The following lemma therefore follows.

Lemma 9.1. *If p is a prime dividing neither $\Delta(u)$ nor D, then the restricted period τ of (u) modulo p is the least common multiple of the numbers $\sigma_1, \sigma_2, \cdots, \sigma_l$ associated with the congruence* (9.1) *above.*

10. Since $u_n = \beta_1\alpha_1 + \cdots + \beta_k\alpha_k^n$ and the α_i are distinct,

$$\beta_i = u(\alpha_i)/f'(\alpha_i) \neq 0, \qquad (i = 1, \cdots, k). \tag{10.1}$$

Here $u(x)$ is the generator of the sequence (u) and $f'(x)$ the derivative of $f(x)$. Since $D=f'(\alpha_1)f'(\alpha_2)\cdots f'(\alpha_k)$, every prime ideal factor of the denominators of the β_i divides D. Let p be a rational prime. Since $\Delta(u)=\beta_1\beta_2\cdots\beta_k D$ $=u(\alpha_1)u(\alpha_2)\cdots u(\alpha_k)$ we can state

LEMMA 10.1. *If* $(p, D)=(p, \beta_1\beta_2\cdots\beta_k)=1$, *then* $(p, \Delta(u))=1$. *Conversely if* $(p, \Delta(u))=(p, D)=1$, *then* $(p, \beta_1\beta_2\cdots\beta_k)=1$, *$p$ a rational prime.*

Form the k sets of sums of the β taken $1, 2, \cdots, k$ at a time:

$$(10.2)\qquad \beta_1+\beta_2+\cdots+\beta_i, \cdots, \beta_{k-i+1}+\beta_{k-i+2}+\cdots+\beta_k,$$

where $(i=1, 2, \cdots, k)$, and each set contains ${}_kC_i$ summands, not necessarily all distinct. Then take the symmetric products over each set

$$\mathrm{B}_i=\prod(\beta_1+\beta_2+\cdots+\beta_i)\qquad (i=1, 2, \cdots, k;\ \mathrm{B}_k=0).$$

Finally let $B=B(u)=\mathrm{B}_1\mathrm{B}_2\cdots\mathrm{B}_{k-1}$. Then B is a rational number of the form P/Q, where P and Q are integers, co-prime if $B\neq 0$ and the only primes dividing Q are divisors of D.

THEOREM 10.1. *If a prime p divides neither numerator nor denominator of B, its rank of apparition is the restricted period of (u) modulo p.*

By Lemma 10.1 any such prime p satisfies the hypothesis of Lemma 9.1. Let $\mathfrak{p}$ be any prime ideal factor of p, and ρ the rank of apparition of p. Since $p\mid u_\rho$ implies that $p\mid u_{n\rho}$,

$$(10.3)\quad \beta_1\alpha_1^{n\rho}+\beta_2\alpha_2^{n\rho}+\cdots+\beta_k\alpha_k^{n\rho}\equiv 0 \pmod{\mathfrak{p}}\qquad (n=0, 1, \cdots, k-1).$$

Since the β_i are integers modulo $\mathfrak{p}$ and prime to $\mathfrak{p}$, the determinant of this set of congruences is divisible by $\mathfrak{p}$. But this determinant is the difference product of the numbers $\alpha_1^\rho, \alpha_2^\rho, \cdots, \alpha_k^\rho$. Hence these numbers are not all distinct modulo p. *I say that*

$$(10.4)\qquad \alpha_1^\rho\equiv\alpha_2^\rho\equiv\cdots\equiv\alpha_k^\rho \pmod{\mathfrak{p}}.$$

Otherwise the numbers can be grouped into two or more sets:

$$\alpha_{i_1}^\rho\equiv\alpha_{i_2}^\rho\equiv\cdots\equiv\alpha_{i_s}^\rho\equiv\zeta_1 \pmod{\mathfrak{p}}$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\alpha_{j_1}^\rho\equiv\alpha_{j_2}^\rho\equiv\cdots\equiv\alpha_{j_t}^\rho\equiv\zeta_m \pmod{\mathfrak{p}}$$

such that the ζ are all distinct modulo p. The congruences (10.3) can then be replaced by

$$\beta_1'\zeta_1^n+\beta_2'\zeta_2^n+\cdots+\beta_m'\zeta_m^n\equiv 0 \pmod{\mathfrak{p}},$$

where the β' occur in the sets (10.2) of sums of β's. The determinant of the first m of these congruences as the difference product of the ζ is prime to $\mathfrak{p}$. Thus $\beta_1' \equiv \beta_2' \equiv \cdots \equiv \beta_m' \equiv 0 \pmod{\mathfrak{p}}$, so that $p \mid B$, contrary to hypothesis.

From (10.4) and the definition of the numbers σ in §9, we see that $\sigma \mid \rho$. Since this argument applies to all of the prime ideal factors of p, the least common multiple of $\sigma_1, \cdots, \sigma_l$ divides ρ. That is, by Lemma 9.1, $\tau \mid \rho$. But ρ always divides τ[2]. Hence $\rho = \tau$.

LEMMA 10.1. *If the number $B = B(u)$ is not zero, the rank of apparition of all save a finite number of primes in (u) is their restricted period.*

11. We now prove

THEOREM 11.1. *A sufficient condition that the number B be not zero is that the group of the characteristic polynomial of (u) be either alternating or symmetric.*

If B vanishes, one of the numbers of the set (10.2) vanishes. With a proper choice of notation we may assume that*

$$\beta_1 + \beta_2 + \cdots + \beta_i = 0, \qquad (k/2 \leqq i \leqq k). \tag{11.1}$$

We may also assume that $k > 4$, as the cases $k = 2, 3, 4$ may be easily discussed directly (see next theorem). Hence $i \geqq 3$.

If we represent the Galois group $\mathfrak{G}$ of $f(x)$ as a permutation group upon the k roots $\alpha_1, \cdots, \alpha_k$, then formula (10.1) shows that any permutation of the α induces the corresponding permutation upon the β. If $\mathfrak{G}$ is alternating or symmetric, it contains the permutation $S = (\alpha_1\alpha_{i+1})(\alpha_2\alpha_3)$. On applying S to (11.1), we obtain $\beta_{i+1} + \beta_2 + \beta_3 + \cdots + \beta_i = 0$. Hence $\beta_1 = \beta_{i+1}$. Similarly, $\beta_2 = \beta_{i+1}, \cdots, \beta_i = \beta_{i+1}$. Hence $\beta_{i+1} = 0$ contrary to (10.1).

The following result is proved by similar reasoning.

THEOREM 11.2. *For low orders of (u), sufficient conditions that $B(u) \neq 0$ are as follows:*

Order of (u)	*Condition of Galois group or characteristic polynomial*
2, 3	*none*
4	*order of group divisible by* 3
5	*$f(x)$ irreducible, or product of an irreducible quartic and linear factor*
6, 7	*group transitive and primitive.*

* It will be recalled that $\beta_1 + \beta_2 + \cdots + \beta_k = u_0 = 0$.

References

1. Annals of Mathematics, (2), vol. 18 (1916–17), pp. 51–64.

2. American Journal of Mathematics, vol. 58 (1936), pp. 577–584.

3. Duke Mathematical Journal, vol. 2 (1936), pp. 472–476.

4. These Transactions, vol. 35 (1933), pp. 600–628.

5. R. D. Carmichael, Quarterly Journal of Mathematics, vol. 48 (1920), pp. 343–372.

6. Bulletin de la Sciences Physiques Mathématiques de Kazan, (2), vol. 12 (1902), pp. 33–49. (In Russian.)

7. S. Lubelski, Crelle's Journal, vol. 102 (1930), pp. 66–67.

8. S. Lubelski, Prace Matematyczno-Fizyczne, vol. 43 (1936), p. 214.

9. Hilbert, *Die Theorie der algebraischen Zahlkörper*, Works, vol. 1, p. 85, Theorem 31; p. 144, Theorem 85.

California Institute of Technology,
Pasadena, Calif.