ON THE POWERS OF A REAL NUMBER REDUCED MODULO ONE

BY

FRED SUPNICK, H. J. COHEN AND J. F. KESTON

1. **Introduction.** Let us consider the sequence

$$(1.1)\qquad \alpha - [\alpha],\quad \alpha^2 - [\alpha^2],\quad \alpha^3 - [\alpha^3], \cdots,$$

where α is a real number greater than one ($[x]$ denotes the greatest integer(1) less than or equal to x). It has been shown by Koksma (cf. [1]) that the terms of (1.1) distribute uniformly on the interval (0, 1) for almost all $\alpha > 1$. We note, however, that the elements of (1.1) need not be distinct (e.g. α integral, or $\alpha = 2^{1/2}$).

Consider all the values $v_1, v_2, v_3, \cdots$ ($v_i \neq v_j$ for $i \neq j$) assumed at least once by the terms of (1.1). Let us denote the set of all positive integers i such that $\alpha^i - [\alpha^i] = v_1$ by C_1, the set of all positive integers i such that $\alpha^i - [\alpha^i] = v_2$ by C_2, etc. That is, the set $\mathcal{J}$: $\{1, 2, \cdots, n, \cdots\}$ partitions into sets $C_1, C_2, \cdots$:

$$(1.2)\qquad \mathcal{J} = C_1 + C_2 + C_3 + \cdots$$

with the property that $j, k \in C_\nu$ if and only if

$$\alpha^j - [\alpha^j] = \alpha^k - [\alpha^k],$$

i.e. if and only if

$$(1.3)\qquad \alpha^k - \alpha^j = r,$$

r integral. The set $\{C_1, C_2, C_3, \cdots\}$ will be denoted by $\mathcal{J}/\alpha$, and will be called the *decomposition of* $\mathcal{J}$ *induced by* α.

In this paper we study the decomposition $\mathcal{J}/\alpha$ for $\alpha > 1$.

The elements C_ν of $\mathcal{J}/\alpha$ will be called *exponent classes*. If an exponent class contains only one element of $\mathcal{J}$, it will be called *unitary*; if each C_ν is unitary, then $\mathcal{J}/\alpha$ will be referred to as a *unitary decomposition.*

$\mathcal{J}/\alpha$ is unitary if and only if the equation (1.3) has no solutions in positive integers j, k, r. Thus if α is not an algebraic integer, the decomposition is unitary (cf. [2]). Therefore we consider only *integral algebraic* α.

If α is a rational integer, the problem is trivial. Therefore we consider only *irrational integral algebraic* α.

Let the minimal polynomial of α be

Presented to the Society, October 26, 1957; received by the editors February 25, 1959.

(1) The term "integer" not preceded by "algebraic" will mean "rational integer."

$$M_\alpha(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n,$$

where the a_i are integers. If a_n is positive, $M_\alpha(x)$ has at least one positive zero other than α and hence $M_\alpha(x)$ cannot divide any polynomial of the form $x^k - x^j - r$, where j, k, r are positive integers with j less than k (since any polynomial of this form has only one positive zero). Thus, if a_n is positive, α cannot satisfy any relation of the form (1.3) and so the decomposition is unitary. Therefore we consider only *irrational integral algebraic α whose minimal polynomial has a negative constant term.*

We let $L(\alpha)$ denote the number of nonzero terms in $M_\alpha(x)$.

If an exponent class contains exactly two elements, it will be called *binary.*

Summary of main results. For $L(\alpha)=2$, 3 the complete decompositions $\mathcal{I}/\alpha$ are obtained (cf. Theorems 1 and 7, §2). For $L(\alpha)\geqq 3$, we prove (i) that each C_ν is either unitary or binary, and (ii) that at most a finite number of the C_ν are binary (cf. Theorems 2 and 3, §2). Sufficient conditions for unitary decomposition are obtained in Corollary 5.1 and Theorems 4, 5 and 6 (cf. §2).

2. **Statement of results.** In the following theorems α is understood to be a real irrational algebraic integer greater than unity whose minimal polynomial has a negative constant term.

THEOREM 1. *Suppose $L(\alpha)=2$; that is, $M_\alpha(x)=x^n-K$, where $K>0$. Then the set $\{n, 2n, 3n, \cdots\}$ comprises a single exponent class C_{ν_0} of $\mathcal{I}/\alpha$, while each positive integer not belonging to C_{ν_0} forms a unitary exponent class (cf. §3).*

THEOREM 2. *If $L(\alpha)\geqq 3$, then no C_ν can contain more than two elements (cf. §4).*

LEMMA 5.1[2]. *Let $L(\alpha)\geqq 3$, and suppose that (j, k) is a binary exponent class of $\mathcal{I}/\alpha$, where $j<k$. Then,*

$$0 < \frac{\alpha^n - |a_n|}{\alpha^n} \leqq \frac{1}{\alpha^{k-j}}, \tag{2.1}$$

where a_n denotes the (negative) constant term of $M_\alpha(x)$ (cf. §5).

COROLLARY 5.1. *Let $L(\alpha)\geqq 3$, and suppose that $a_i \geqq 0$ in $M_\alpha(x)$, for $1\leqq i \leqq n-1$. Then $\mathcal{I}/\alpha$ is unitary.*

COROLLARY 5.2. *Let $L(\alpha)\geqq 3$, and suppose that $\mathcal{I}/\alpha$ is nonunitary. Then,*

$$\alpha^{n-1}(\alpha - 1) \leqq |a_n| < \alpha^n. \tag{2.2}$$

COROLLARY 5.3. *Let $L(\alpha)\geqq 3$, and suppose that $\mathcal{I}/\alpha$ is nonunitary. Let the roots of $M_\alpha(x)$ be denoted by $z_1, z_2, \cdots, z_n$. Then,*

(2) Integral parts of lemma-numbers indicate sections containing proofs; corollary-numbers have same integral parts as the theorem or lemma to which they are attached.

$$\alpha - 1 \leqq |z_i| \leqq \alpha \qquad (i = 1, 2, \cdots, n). \tag{2.3}$$

THEOREM 3. *For any $\mathcal{I}/\alpha$, at most a finite number of the C_ν are binary (cf. §6).*

We note that Theorems 1, 2 and 3 jointly imply the following statement: *Let α be a real number greater than one. Then, the equation $\alpha^x - \alpha^y = z$ has at most a finite number of solutions in positive integers x, y, z, except in the case when $\alpha = K^{1/n}$, where n, K are positive integers*(3).

Theorems 4, 5 and 6 state sufficient conditions for unitary decomposition.

THEOREM 4. *Suppose*

$$M_\alpha(x) = x^n - b_1x^{n-1} - b_2x^{n-2} - \cdots - b_{n-1}x - b_n, \tag{2.4}$$

where each $b_i \geqq 0$, and $\sum_{i=1}^{n-1} b_i > 1$. Then $\mathcal{I}/\alpha$ is unitary (cf. §7).

COROLLARY 4.1. *Let $M_\alpha(x)$ be of form (2.4) where each $b_i \geqq 0$. Then, if $L(\alpha) \geqq 4$, $\mathcal{I}/\alpha$ is unitary.*

THEOREM 5. *Suppose $M_\alpha(x)$ is of the form*

$$M_\alpha(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x - 1,$$

where $\sum_{i=1}^{n-1} a_i \neq -1$. Then $\mathcal{I}/\alpha$ is unitary (cf. §8).

THEOREM 6. *If $M_\alpha(x)$ has two real roots of the same sign, then $\mathcal{I}/\alpha$ is unitary (cf. §9).*

Theorem 7 states the complete decomposition for the case $L(\alpha) = 3$.

THEOREM 7. *Let $M_\alpha(x) = x^n + ax^{n-r} - K$, $(a \neq 0, K > 0, 0 < r < n)$.*

(a) *If $a \neq -1$, then $\mathcal{I}/\alpha$ is unitary.*

(b) *If $a = -1$, then the integers $(n-r, n)$ form a binary class, by definition. There will be no other binary classes, unless $M_\alpha(x)$ is of the special form:*

$$M_\alpha(x) = x^{3t} - x^t - 1. \tag{2.5}$$

In this exceptional case, each of the pairs $(t, 3t)$ and $(4t, 5t)$ forms a binary class, and there are no others (cf. §10).

3. **Proof of Theorem** 1. We assume $n > 1$. The integers $(n, 2n, 3n, \cdots)$ clearly belong to the same exponent class C_{ν_0}. If $m = an + b$, where $a \geqq 0$ and $0 < b < n$, then m *cannot* belong to C_{ν_0}. Otherwise, we would have

$$\alpha^{an+b} - \alpha^n = t,$$

where t is integral; but this becomes

(3) A theorem of A. Gelfond (cf. [3]) contains, as a special case, an analogous result for the closely related equation $\alpha^x - \alpha^y = \delta^z$, where α, δ are given real, algebraic numbers.

$$K^a\alpha^b - K = t,$$

which is of lower degree in α than the degree n of $M_\alpha(x)$. Thus the integers $(n, 2n, 3n, \cdots)$ comprise the *complete* class C_{r_0}.

Suppose

$$r = a_1n + b_1, \qquad s = a_2n + b_2,$$

where $a_i \geqq 0$ and $0 < b_i < n$, $(i = 1, 2)$, and assume that r and s were in the same class. We would then have

$$\alpha^{a_1n+b_1} - \alpha^{a_2n+b_2} = t,$$

or,

$$K^{a_1}\alpha^{b_1} - K^{a_2}\alpha^{b_2} - t = 0,$$

which, as before, is impossible unless r equals s.

4. **Proof of Theorem** 2. We first prove

LEMMA 4.1. *If $M_\alpha(x)$ has a root β such that $|\beta| < 1$, then no exponent class in $\mathcal{I}/\alpha$ can contain more than two elements.*

Proof. Suppose the integers j, k belong to the same exponent class, where $j < k$. That is,

$$\alpha^k - \alpha^j = r,$$

where r is a positive integer. Then, since $M_\alpha(x)$ must divide $x^k - x^j - r$,

$$\beta^k - \beta^j = r.$$

Therefore

$$r \leqq |\beta|^k + |\beta|^j < 2.$$

Hence $r = 1$. Thus, if some exponent class contained *three* elements $u < v < w$, we would then have

$$\alpha^w - \alpha^u = 1,$$

and

$$\alpha^w - \alpha^v = 1.$$

But these relations imply $\alpha^u = \alpha^v$, which is impossible.

Proof of Theorem 2. We now assume, in view of Lemma 4.1, that no root of $M_\alpha(x)$ has absolute value less than unity.

If the theorem were false, there would exist three positive integers $j < k < m$, such that

$$\alpha^k - \alpha^j = r, \tag{4.1}$$

and

$$\alpha^m - \alpha^j = s, \tag{4.2}$$

where r, s are positive integers, $r<s$. Let us write the n roots $z_1, z_2, \cdots, z_n$ of $M_\alpha(x)$ in the form

$$z_\nu = \rho_\nu e^{i\theta_\nu}, \qquad (\nu = 1, 2, \cdots, n), \tag{4.3}$$

where each $\rho_\nu \geqq 1$.

Now from (4.1),

$$x^k - x^j - r = M_\alpha(x)\cdot P(x), \tag{4.4}$$

where $P(x)$ is a polynomial with integral coefficients. We note that if $|x| > \alpha$, then

$$|x^k - x^j| \geqq |x|^k - |x|^j > \alpha^k - \alpha^j = r; \tag{4.5}$$

thus no zero of $x^k - x^j - r$ has absolute value greater than α. Since the left member of (4.4) has each z_ν among its roots, then

$$1 \leqq \rho_\nu \leqq \alpha, \qquad (\nu = 1, 2, \cdots, n). \tag{4.6}$$

We will now prove that each $\rho_\nu = \alpha$, $(\nu = 1, 2, \cdots, n)$. Substituting (4.3) into (4.4), we have

$$r = \rho_\nu^k \cos k\theta_\nu - \rho_\nu^j \cos j\theta_\nu,$$
$$0 = \rho_\nu^k \sin k\theta_\nu - \rho_\nu^j \sin j\theta_\nu.$$

Transposing the second term of each right member to the left, squaring each equation, and adding, we obtain

$$r^2 + 2r\rho_\nu^j \cos j\theta_\nu + \rho_\nu^{2j} = \rho_\nu^{2k}. \tag{4.7}$$

Similarly, from (4.2),

$$s^2 + 2s\rho_\nu^j \cos j\theta_\nu + \rho_\nu^{2j} = \rho_\nu^{2m}. \tag{4.8}$$

Eliminating θ_ν between (4.7) and (4.8),

$$r^2 s - s^2 r + s\rho_\nu^{2j} - r\rho_\nu^{2j} = s\rho_\nu^{2k} - r\rho_\nu^{2m}.$$

Thus, defining the polynomial

$$G(x) = rx^{2m} - sx^{2k} + (s - r)x^{2j} - rs(s - r), \tag{4.9}$$

we have

$$G(\rho_\nu) = 0, \qquad (\nu = 1, 2, \cdots, n). \tag{4.10}$$

From (4.9), using (4.1) and (4.2), we obtain

$$G(0) = G(1) = G(\alpha^{1/2}) = -rs(s - r) < 0.$$

Therefore, there exist x_0, x_1, $0<x_0<1$, $1<x_1<\alpha^{1/2}$, such that

$$G'(x_0) = G'(x_1) = 0.$$

But, since $G'(x)$ is a trinomial, it has at most two positive roots, which must then be x_0, x_1. Moreover, since the leading coefficient of $G'(x)$ is positive, we have

$$G'(x) > 0 \qquad \text{for } x > x_1.$$

That is, $G(x)$ is *strictly increasing* for $x>x_1$. But $G(\alpha)=0$, and $x_1<\alpha$. Therefore, $G(x)<0$ for $x_1 \leqq x<\alpha$. We now show that $G(x)<0$ for $1<x<x_1$. Assume that $G(x_2)\geqq 0$, where $1<x_2<x_1$. Since $G(1)$ and $G(x_1)$ are each negative, this would imply that $G'(x)$ has a root *between* 1 and x_1, which is impossible. We thus have

$$G(x) < 0 \qquad \text{for } 1 \leqq x < \alpha. \tag{4.11}$$

Therefore, from (4.11), (4.10), and (4.6), we conclude

$$\rho_\nu = \alpha, \qquad (\nu = 1, 2, \cdots, n).$$

Now, taking the product of the absolute values of the roots (4.3) of $M_\alpha(x)$, we obtain

$$\alpha^n = |a_n|, \tag{4.12}$$

which contradicts the assumption that $L(\alpha)\geqq 3$. This completes the proof of Theorem 2.

5. **Proof of Lemma** 5.1. Let $\alpha^k - \alpha^j = r$. Then

$$x^k - x^j - r = M_\alpha(x)\cdot P(x), \tag{5.1}$$

where $P(x)$ is a polynomial of degree $(k-n)$, having integral coefficients. Denote the roots of $M_\alpha(x)$ by $z_1, z_2, \cdots, z_n$, and those of $P(x)$ by $\omega_1, \omega_2, \cdots, \omega_{k-n}$. Since the left member of (5.1) has each z_i among its roots and α as its unique positive root, we then have (cf. (4.5))

$$|z_i| \leqq \alpha, \qquad (i = 1, 2, \cdots, n); \tag{5.2}$$

similarly,

$$|\omega_i| \leqq \alpha, \qquad (i = 1, 2, \cdots, k-n). \tag{5.3}$$

Therefore, by (5.2), we get

$$|a_n| = |z_1|\cdot|z_2| \cdots |z_n| \leqq \alpha^n. \tag{5.4}$$

The right equality sign in (5.4) cannot hold, since $L(\alpha)\geqq 3$. Thus, the left inequality of (2.1) holds.

From (5.1),

$$\alpha^k - \alpha^j = r = |z_1| \cdot |z_2| \cdots |z_n| \cdot |\omega_1| \cdot |\omega_1| \cdots |\omega_{k-n}|,$$

and therefore, by (5.3),

$$\alpha^k - \alpha^j \leqq |a_n| \alpha^{k-n}. \tag{5.5}$$

The right inequality of (2.1) is simply a rearrangement of (5.5). This completes the proof of Lemma 5.1.

REMARK 1. We show that *the equality sign in* (2.1) *holds if and only if*

$$M_\alpha(x) = x^k - x^j - |a_k|.$$

Sufficiency. Assume that $M_\alpha(x) = x^k - x^j - |a_k|$. Then

$$\frac{\alpha^n - |a_n|}{\alpha^n} = \frac{\alpha^k - |a_k|}{\alpha^k} = \frac{\alpha^j}{\alpha^k} = \frac{1}{\alpha^{k-j}}.$$

Necessity. Assume that

$$\frac{\alpha^n - |a_n|}{\alpha^n} = \frac{1}{\alpha^{k-j}}.$$

Since (j, k) is an exponent class, $\alpha^k - \alpha^j = r$ (a positive integer), where $k \geqq n$. Now,

$$\frac{\alpha^n - |a_n|}{\alpha^n} = \frac{\alpha^j}{\alpha^k} = \frac{\alpha^k - r}{\alpha^k}. \tag{5.6}$$

Equating the first and third expressions in (5.6), we obtain

$$|a_n| \alpha^k = r\alpha^n. \tag{5.7}$$

If $k \neq n$, $\alpha^{k-n} = r/|a_n|$, contradicting the hypothesis that $L(\alpha) \geqq 3$ (cf. §6' Lemma 6.1). Thus $n = k$, and from (5.7), $r = |a_n|$. Therefore $M_\alpha(x) = x^k - x^j - |a_k|$.

Proof of Corollary 5.1. If $\mathfrak{g}/\alpha$ were not unitary, we would have

$$0 < \alpha^n - |a_n| = -a_1\alpha^{n-1} - a_2\alpha^{n-2} - \cdots - a_{n-1}\alpha < 0,$$

which is impossible.

Proof of Corollary 5.2. We need prove only the left inequality. Thus, if (j, k) is a binary class, with $j < k$,

$$\alpha^{n-1}(\alpha - 1) \leqq \alpha^n - \alpha^{n-(k-j)} \leqq |a_n|,$$

by (2.1).

Proof of Corollary 5.3. The right inequality is the same as (5.2). To prove the left inequality, we have

$$\begin{aligned} \alpha^{n-1}(\alpha - 1) &\leqq |a_n| \\ &= |z_1| \cdot |z_2| \cdots |z_n| \\ &\leqq \alpha^{n-1} |z_i|. \end{aligned}$$

Dividing by α^{n-1}, we obtain the desired result.

REMARK 2. The following example shows that the left equality sign in (2.3) may hold for some of the conjugates of certain α:

$$M_\alpha(x) = x^2 - x - K$$

$(K>0)$ has α and $1-\alpha$ $(\alpha>1)$ as roots.

6. **Proof of Theorem** 3. We first prove

LEMMA 6.1. *If there exists a positive integer t such that α^t is rational, then* $L(\alpha)=2$.

Proof. Let h denote the *smallest* positive integer such that α^h is rational; let $\alpha^h=v$. Since α is an algebraic integer, v must be integral. We will show that $M_\alpha(x)=x^h-v$, by proving that the binomial x^h-v is irreducible.

If x^h-v were reducible, then $v=b^c$ (cf. [4]), where b, c are positive integers, $c>1$, and c divides h. But, letting $h=rc$,

$$v = \alpha^h = \alpha^{rc} = b^c.$$

This implies $\alpha^r=b$, contradicting the definition of h.

LEMMA 6.2. *Let $L(\alpha)\geqq 3$. Suppose that each of the pairs (j, k), (j', k') forms a binary class of $\mathcal{J}/\alpha$ $(j<k, j'<k')$. Then,*

$$k - j \neq k' - j'.$$

Proof. Assume that $k-j=k'-j'$. Take $k<k'$, and let

$$t = k' - k = j' - j.$$

Then,

$$\alpha^t(\alpha^k - \alpha^j) = \alpha^{k'} - \alpha^{j'},$$

or,

$$\alpha^t = \frac{\alpha^{k'} - \alpha^{j'}}{\alpha^k - \alpha^j} = \frac{u}{v}, \tag{6.1}$$

where u, v are positive integers. Consequently $L(\alpha)=2$, by Lemma 6.1, contradicting the hypothesis.

Proof of Theorem 3. We may assume that $L(\alpha)\geqq 3$, in view of Theorem 1.

Let (j, k) be *any* binary class of $\mathcal{J}/\alpha$ $(j<k)$. The right inequality of (2.1) implies that

$$k - j \leqq n - \log_\alpha (\alpha^n - |a_n|). \tag{6.2}$$

Denoting by N the greatest integer less than or equal to the right member of (6.2), we thus have

$$k - j \leqq N. \tag{6.3}$$

Thus, by Lemma 6.2, there are at most N binary classes.

REMARK 1. *If* $L(\alpha)\geqq 3$, *then* $\mathfrak{g}/\alpha^p$ *is unitary for each positive integer* p *satisfying*:

$$p > [n - \log_\alpha (\alpha^n - |a_n|)] = N.$$

Proof. If this statement were false, there would exist a positive integer $p_0 > N$, and positive integers r, s $(r < s)$ such that

$$(\alpha^{p_0})^s - (\alpha^{p_0})^r$$

is integral. Thus the integers $(p_0 r, p_0 s)$ form a binary class for $\mathfrak{g}/\alpha$. But,

$$p_0 s - p_0 r = p_0(s - r) > N,$$

contradicting (6.3).

REMARK 2. If $\mathfrak{g}/\alpha$ is unitary, then $\mathfrak{g}/\alpha^p$ is also unitary for *all* integers $p \geqq 1$.

7. **Proof of Theorem** 4. Let C_0 be any exponent class of $\mathfrak{g}/\alpha$, and let m denote its smallest element. We show that *no integer larger than* m *can belong to* C_0.

Let the canonical form of α^m (i.e. α^m expressed in terms of the basis $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ with integral coefficients) be given by

$$\alpha^m = c_1\alpha^{n-1} + c_2\alpha^{n-2} + \cdots + c_{n-1}\alpha + c_n, \tag{7.1}$$

where each $c_i \geqq 0$, since each $b_i \geqq 0$. Now, for each positive integer t, we shall denote by S_t the sum of all the coefficients in the canonical form of α^t, excluding the "constant" (i.e. α-free) term, if any. Since (7.1) yields

$$\alpha^{m+1} = (c_1b_1 + c_2)\alpha^{n-1} + (c_1b_2 + c_3)\alpha^{n-2} + \cdots + (c_1b_{n-1} + c_n)\alpha + c_1b_n,$$

we obtain

$$S_{m+1} = S_m + c_n + c_1\left(\left(\sum_{i=1}^{n-1} b_i\right) - 1\right). \tag{7.2}$$

CASE I. Assume that at least one of the integers c_1, c_n is positive. Then, from (7.2), $S_{m+1} > S_m$. Moreover, since S_t is clearly a nondecreasing function of t, we conclude that $S_t > S_m$ for *each* $t > m$. Thus, if $t > m$, α^t cannot have the same canonical form (excluding the "constant" term) as α^m. Therefore, it is impossible that $\alpha^t = \alpha^m + K$, where K is a positive integer.

CASE II. $c_1 = c_n = 0$. Let c_q be the first nonzero coefficient in (7.1). We then have

$$\begin{aligned}
\alpha^m &= c_q\alpha^{n-q} + c_{q+1}\alpha^{n-q-1} + \cdots + c_{n-1}\alpha,\\
\alpha^{m+1} &= c_q\alpha^{n-q+1} + c_{q+1}\alpha^{n-q} + \cdots + c_{n-1}\alpha^2,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
\alpha^{m+q-1} &= c_q\alpha^{n-1} + c_{q+1}\alpha^{n-2} + \cdots + c_{n-1}\alpha^q.
\end{aligned} \tag{7.3}$$

Since the above canonical forms are of ascending degrees, it follows that none of the integers

$$m+1,\ m+2,\ \cdots,\ m+q-1$$

belongs to C_0. Now, just as we obtained (7.2), we can write:

$$S_{m+q} = S_{m+q-1} + c_q\left(\left(\sum_{i=1}^{n-1} b_i\right) - 1\right).$$

But, $S_{m+q-1} = S_m$, from the first and last equations of (7.3). Thus, $S_{m+q} > S_m$, since $c_q > 0$. Hence, as before, no integer larger than m can belong to C_0.

8. **Proof of Theorem** 5. Assume that there exists a binary class (j, k); that is,

$$\alpha^k - \alpha^j = r, \tag{8.1}$$

where r is a positive integer. But, since the constant term of $M_\alpha(x)$ is -1, the product of its roots is ± 1. Hence, since $\alpha > 1$, it follows that $M_\alpha(x)$ must have a root β such that $|\beta| < 1$. We then conclude, as in the proof of Lemma 4.1, that $r = 1$. From (8.1),

$$x^k - x^j - 1 = M_\alpha(x) \cdot P(x), \tag{8.2}$$

where $P(x)$ is a polynomial with integral coefficients. Letting $x = 1$,

$$P(1) = -\frac{1}{M_\alpha(1)}.$$

Therefore, since $P(1)$ must be integral, it follows that $M_\alpha(1) = \pm 1$. Now, $M_\alpha(1)$ cannot be positive; otherwise $M_\alpha(x)$ would have a root between 0 and 1, whereas the left member of (8.2) has only one positive root, namely α.

We thus conclude that

$$\sum_{i=1}^{n-1} a_i = M_\alpha(1) = -1,$$

which contradicts the hypothesis. This completes the proof.

9. **Proof of Theorem 6.** It is sufficient to show that $R(x) = x^k - x^j - r$ cannot have two zeros of the same sign for any pair of values of j, k with $0 < j < k$. Since $R(x)$ has one variation in sign, $R(x)$ has exactly one positive zero. If k is even, $R(-x)$ has one variation in sign and therefore $R(x)$ has exactly one negative zero. If k is odd, $R(x) < -r < 0$ when $x < -1$ and $R(x) < -x^j - r < 0$ when $-1 < x < 0$, so that $R(x)$ has no negative zeros in this case.

10. **Proof of Theorem** 7. If $a < -1$, it follows from Theorem 4 that $\mathfrak{g}/\alpha$ is unitary. If $a > 0$, it follows from Corollary 5.1 that $\mathfrak{g}/\alpha$ is unitary. This proves part (a).

Proof of Theorem 7(b). In this case, we are concerned with a minimal polynomial of the form

$$M_\alpha(x) = x^n - x^{n-r} - K, \tag{10.1}$$

where $K>0$. Thus, the integers $n-r$ and n form a binary class, which we shall refer to as the *trivial* binary class. When (10.1) is of the special form

$$M_\alpha(x) = x^{3t} - x^t - 1, \tag{10.2}$$

the existence of the nontrivial binary class $(4t, 5t)$ follows from the identity

$$(x^{5t} - x^{4t} - 1) = (x^{3t} - x^t - 1)(x^{2t} - x^t + 1). \tag{10.3}$$

In order to complete the proof of Theorem 7(b), we must show that the class $(4t, 5t)$, associated with the minimal polynomial (10.2), is the *only case of a nontrivial binary class* arising from a minimal polynomial of the form (10.1).

We begin by establishing

LEMMA 10.1. *Suppose that $M_\alpha(x)$ is of the form* (10.1). *Then, the positive integer p will be the smaller element of a nontrivial binary class if and only if the canonical form of α^p is of type*

$$\alpha^p = c\alpha^{n-q} + c\alpha^{n-2q} + c\alpha^{n-3q} + \cdots + c\alpha^{n-mq}, \tag{10.4}$$

where $c>0$, $mq=r$, $m>1$. Moreover, the larger element of this binary class must be $(p+q)$.

Proof. The sufficiency is immediate, since (10.4) implies

$$\begin{aligned}\alpha^{p+q} &= c\alpha^{n-q} + c\alpha^{n-2q} + \cdots + c\alpha^{n-mq} + cK \\ &= \alpha^p + cK.\end{aligned}$$

For the necessity, we assume that p is the smaller element of a nontrivial binary class C_0, and denote the canonical form of α^p by

$$\alpha^p = c_q\alpha^{n-q} + c_{q+1}\alpha^{n-q-1} + c_{q+2}\alpha^{n-q-2} + \cdots + c_{n-1}\alpha + c_n, \tag{10.5}$$

all $c_i \geqq 0$, $c_q>0$, $q \geqq 1$. We note that $c_n=0$; otherwise, as in the proof of Theorem 4, Case I, we would have: $S_t > S_p$, for each $t>p$, so that p could not be the smaller element of a binary class.

From (10.5), we see that $\alpha^{p+1}, \alpha^{p+2}, \cdots, \alpha^{p+q-1}$ will each have canonical forms of degree *higher* than $(n-q)$, so that none of the integers $p+1$, $p+2$, $\cdots$, $p+q-1$ can belong to C_0. Moreover, since α^{p+q} will contain the "constant" term c_qK in its canonical form, no integer larger than $(p+q)$ can belong to C_0 (cf. Theorem 4, Case I). Thus, *the second element of C_0 must be* $(p+q)$.

By the "pure-canonical" form of α^w (w integral), we shall mean the canonical form of α^w with all zero terms omitted. We note that the pure-canonical form of α^w $(w \geqq 0)$ has all positive coefficients if $M_\alpha(x)$ is of the form (10.1).

We next show that each exponent in the pure-canonical form of α^p must be of form $(n-aq)$, where "a" is a positive integer. Assume that this is not the case, and let u be the *largest* exponent which is *not* of this form. Suppose that u falls between $(n-bq)$ and $(n-(b+1)q)$, where b is a positive integer. But then, α^{p+q} would contain the exponent $(u+q)$ in its pure-canonical form, while α^p does not, which is impossible.

Moreover, since α^{p+q} contains the exponent $(n-r)$ in its pure-canonical form, so must α^p; hence, $r=mq$, $m\geqq 1$. Thus (10.5) becomes

$$\alpha^p = c_q\alpha^{n-q} + c_{2q}\alpha^{n-2q} + \cdots + c_{mq}\alpha^{n-mq} + \cdots + c_{vq}\alpha^{n-vq}, \tag{10.6}$$

where $v\geqq m$, $c_{mq}>0$, $c_{vq}>0$.

We next see that $v=m$. For, if $v>m$, α^{p+q} would not contain the exponent $(n-vq)$ in its pure-canonical form. Thus, (10.6) becomes

$$\alpha^p = c_q\alpha^{n-q} + c_{2q}\alpha^{n-2q} + \cdots + c_{mq}\alpha^{n-mq}, \tag{10.7}$$

where $mq=r$. We can now see that $m>1$; otherwise, we would have

$$\alpha^p = c_q\alpha^{n-r}, \quad \text{or} \quad \alpha^{p-n+r} = c_q,$$

contradicting Lemma 6.1.

Finally, from (10.7) we obtain

$$\alpha^{p+q} = c_{2q}\alpha^{n-q} + C_{3q}\alpha^{n-2q} + \cdots + c_{mq}\alpha^{n-(m-1)q} + c_q\alpha^{n-mq} + c_qK. \tag{10.8}$$

Comparing (10.8) and (10.7), we conclude that

$$c_q = c_{2q} = \cdots = c_{mq},$$

completing the proof of Lemma 10.1.

It will now be shown that if there exists an integer p such that α^p is of form (10.4), then the minimal polynomial (10.1) must be of form (10.2), where $p=4t$, $q=t$. Toward this end, we first establish:

LEMMA 10.2. *If there exists an integer p such that α^p is of form* (10.4), *then* $K=1$ *in* (10.1), *and* $c=1$ *in* (10.4).

Proof. Dividing (10.4) by α^{n-mq}, we have

$$\alpha^{p-n+mq} = c[\alpha^{(m-1)q} + \alpha^{(m-2)q} + \cdots + \alpha^q + 1]. \tag{10.9}$$

Therefore,

$$\begin{aligned} x^{p-n+mq} - c[x^{(m-1)q} + x^{(m-2)q} + \cdots + x^q + 1] \\ = (x^n - x^{n-r} - K)\cdot P(x), \end{aligned} \tag{10.10}$$

where $P(x)$ is a polynomial with integral coefficients. Letting $x=0$ in (10.10), we get: $-c=-K\cdot P(0)$, so that K divides c. Then letting $x=1$ in (10.10), we get: $1-mc=-K\cdot P(1)$, so that K also divides $mc-1$. Since $m>1$, $mc-1\neq 0$; it thus follows that $K=1$.

Since $K=1$, α is a unit in the ring H of algebraic integers. Therefore,

α^{p-n+mq} is also a unit. But, according to (10.9), c must divide α^{p-n+mq} (in H), since the quantity in the bracket is an algebraic integer. Hence, c is a unit, and must be 1.

This completes the proof of Lemma 10.2.

LEMMA 10.3. *If α^p has a canonical form of type* (10.4), *then $n<p<n+r$.*

Proof. It is clear that $n<p$; otherwise, α would satisfy an equation of degree less than n.

Now, since $K=1$, (10.1) becomes

$$\alpha^n = \alpha^{n-r} + 1. \tag{10.11}$$

Therefore,

$$\alpha^{n+r} = \alpha^{n-r} + \alpha^r + 1. \tag{10.12}$$

Suppose first that $n+r \leqq p < 2n$. That is, $p=n+r+s$, where $0 \leqq s < n-r$. The canonical form of α^p can then be obtained by multiplying (10.12) by α^s. Therefore, the terminating exponent in the pure-canonical form of α^p will be *less* than $n-r$, contrary to (10.4).

Next, suppose $p \geqq 2n$. Squaring (10.11),

$$\alpha^{2n} = \alpha^{2(n-r)} + 2\alpha^{n-r} + 1. \tag{10.13}$$

Thus, the canonical form of α^p will have at least one coefficient $\geqq 2$, since $\alpha^p = \alpha^{p-2n} \cdot \alpha^{2n}$ and all coefficients in the canonical form of α^{p-2n} are non-negative integers. But this contradicts (10.4), since $c=1$.

This concludes the proof of Lemma 10.3.

LEMMA 10.4. *If there exists an integer p such that α^p is of form* (10.4), *then $M_\alpha(x)$ must be of form* (10.2), *where $p=4t$ and $q=t$.*

Proof. By Lemma 10.3, we have: $p=n+t$, where $0<t<r$. From (10.11), we obtain

$$\alpha^p = \alpha^{n-(r-t)} + \alpha^t. \tag{10.14}$$

Comparing (10.14) with (10.4), we conclude that $r-t=q$, and $t=n-r=n-2q$. These relations imply that $q=t$, $n=3t$, $r=2t$, so that (10.1) becomes (10.2). Moreover, $p=n+t=4t$.

The proof of Theorem 7 is now complete.

11. **A class of $M_\alpha(x)$ with nonunitary $\mathfrak{g}/\alpha$ and $L(\alpha)>3$.** Consider the class of polynomials of form

$$P(x) = x^{(2r-1)q} - 2x^{(2r-2)q} + 2x^{(2r-3)q} - \cdots + 2x^q - 2,$$

where r and q are positive integers, $r \geqq 2$. We first note that $P(x)$ is irreducible by Eisenstein's Criterion (cf. [5]). Moreover, from the identity

$$(x^q + 1)\cdot P(x) = x^{2rq} - x^{(2r-1)q} - 2, \tag{11.1}$$

we see that $P(x)$ has exactly one positive root α $(1<\alpha<2)$. Thus $P(x)$ is the minimal polynomial of α. Finally, from (11.1), we see that $(2r-1)q$ and $2rq$ form a binary class of $\mathcal{J}/\alpha$.

12. **Some unanswered questions.** The decomposition $\mathcal{J}/\alpha$ has at most a finite number of binary classes, by Theorem 3. However, the authors have no example of an α for which $\mathcal{J}/\alpha$ has *more than two* binary classes; nor do they have an example for which $\mathcal{J}/\alpha$ has *exactly two* binary classes, aside from the case where $M_\alpha(x)$ is of the form $x^{3t}-x^t-1$ (cf. Theorem 7).

We therefore pose the following questions:

(1) Does there exist an α for which $\mathcal{J}/\alpha$ has *more than two* binary classes?

(2) Does there exist an α, other than the case where $M_\alpha(x)$ is of the form $x^{3t}-x^t-1$, for which $\mathcal{J}/\alpha$ has *exactly two* binary classes?

We note that if there exists a t_0 such that $Q(x)=x^{3t_0}-x^{t_0}-1$ is *reducible*, then the positive root α of $Q(x)$ will induce a decomposition $\mathcal{J}/\alpha$ having *at least two* binary classes: $(t_0, 3t_0)$, $(4t_0, 5t_0)$ (cf. (10.3)). Furthermore, for this case, $M_\alpha(x)$ cannot be of the form $x^{3s}-x^s-1$ $(s<t_0)$; otherwise, $\mathcal{J}/\alpha$ would have at least four binary classes: $(s, 3s)$, $(4s, 5s)$, $(t_0, 3t_0)$, $(4t_0, 5t_0)$, contradicting Theorem 7.

REFERENCES

1. J. F. Koksma, *Ein mengentheoretischer Satz über die Gleichverteilung modulo Eins*, Compositio Math. vol. 2 (1935) pp. 250–258.

2. E. Hecke, *Vorlesungen über die Theorie der algebraichen Zahlen*, New York, Chelsea, 1948. cf. Satz 60 p. 78; or H. Pollard, *The theory of algebraic numbers*, New York, Wiley, 1950. Cf. Lemma 6.1, p. 58.

3. A. Gelfond, *Sur la divisibilité de la différence des puissances de deux nombres entiers par une puissance d'un idéal premier*, Mat. Sb. N.S. vol. 7 (1940) pp. 7–25. Cf. Theorem IV, p. 21.

4. K. Th. Vahlen, *Über reductible Binome*, Acta Math. vol. 19 (1895) pp. 195–198.

5. B. L. van der Waerden, *Modern algebra*, vol. 1, New York, Ungar, 1949, p. 74.

CITY COLLEGE,
NEW YORK, NEW YORK