

# 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

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

where  $\alpha$  is a real number greater than one ( $[x]$  denotes the greatest integer<sup>(1)</sup> 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.  $\alpha$  integral, or  $\alpha = 2^{1/2}$ ).

Consider all the values  $v_1, v_2, v_3, \dots$  ( $v_i \neq v_j$  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  $\mathcal{g} : \{1, 2, \dots, n, \dots\}$  partitions into sets  $C_1, C_2, \dots$ :

$$(1.2) \quad \mathcal{g} = C_1 + C_2 + C_3 + \dots$$

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

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

i.e. if and only if

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

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

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

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

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

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

Let the minimal polynomial of  $\alpha$  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."

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

where the  $a_i$  are integers. If  $a_n$  is positive,  $M_\alpha(x)$  has at least one positive zero other than  $\alpha$  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,  $\alpha$  cannot satisfy any relation of the form (1.3) and so the decomposition is unitary. Therefore we consider only *irrational integral algebraic  $\alpha$  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  $\mathcal{G}/\alpha$  are obtained (cf. Theorems 1 and 7, §2). For  $L(\alpha) \geq 3$ , we prove (i) that each  $C_v$  is either unitary or binary, and (ii) that at most a finite number of the  $C_v$  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  $\alpha$  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  $\{n, 2n, 3n, \dots\}$  comprises a single exponent class  $C_{r_0}$  of  $\mathcal{G}/\alpha$ , while each positive integer not belonging to  $C_{r_0}$  forms a unitary exponent class (cf. §3).*

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

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

$$(2.1) \quad 0 < \frac{\alpha^n - |a_n|}{\alpha^n} \leq \frac{1}{\alpha^{k-i}},$$

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

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

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

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

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

---

<sup>(2)</sup> 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.

$$(2.3) \quad \alpha - 1 \leq |z_i| \leq \alpha \quad (i = 1, 2, \dots, n).$$

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

We note that Theorems 1, 2 and 3 jointly imply the following statement: Let  $\alpha$  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<sup>(\*)</sup>.

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

THEOREM 4. Suppose

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

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

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

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

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

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

THEOREM 6. If  $M_\alpha(x)$  has two real roots of the same sign, then  $\mathcal{G}/\alpha$  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  $\mathcal{G}/\alpha$  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:

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

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  $(n, 2n, 3n, \dots)$  clearly belong to the same exponent class  $C_{r_0}$ . If  $m = an + b$ , where  $a \geq 0$  and  $0 < b < n$ , then  $m$  cannot belong to  $C_{r_0}$ . Otherwise, we would have

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

where  $t$  is integral; but this becomes

(\*) 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  $\alpha, \delta$  are given real, algebraic numbers.

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

which is of lower degree in  $\alpha$  than the degree  $n$  of  $M_\alpha(x)$ . Thus the integers  $(n, 2n, 3n, \dots)$  comprise the *complete* class  $C_r$ .

Suppose

$$r = a_1 n + b_1, \quad s = a_2 n + b_2,$$

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

$$\alpha^{a_1 n + b_1} - \alpha^{a_2 n + b_2} = t,$$

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  $\beta$  such that  $|\beta| < 1$ , then no exponent class in  $\mathcal{S}/\alpha$  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

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

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

$$(4.1) \quad \alpha^k - \alpha^j = r,$$

and

$$(4.2) \quad \alpha^m - \alpha^j = s,$$

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

$$(4.3) \quad z_\nu = \rho_\nu e^{i\theta_\nu}, \quad (\nu = 1, 2, \dots, n),$$

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

Now from (4.1),

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

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

$$(4.5) \quad |x^k - x^j| \geq |x|^k - |x|^j > \alpha^k - \alpha^j = r;$$

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

$$(4.6) \quad 1 \leq \rho_\nu \leq \alpha, \quad (\nu = 1, 2, \dots, n).$$

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

$$\begin{aligned} r &= \rho_\nu^k \cos k\theta_\nu - \rho_\nu^j \cos j\theta_\nu, \\ 0 &= \rho_\nu^k \sin k\theta_\nu - \rho_\nu^j \sin j\theta_\nu. \end{aligned}$$

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

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

Similarly, from (4.2),

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

Eliminating  $\theta_\nu$  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

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

we have

$$(4.10) \quad G(\rho_\nu) = 0, \quad (\nu = 1, 2, \dots, n).$$

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

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

That is,  $G(x)$  is *strictly increasing* for  $x > x_1$ . But  $G(\alpha) = 0$ , and  $x_1 < \alpha$ . Therefore,  $G(x) < 0$  for  $x_1 \leq x < \alpha$ . We now show that  $G(x) < 0$  for  $1 < x < x_1$ . Assume that  $G(x_2) \geq 0$ , 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

$$(4.11) \quad G(x) < 0 \quad \text{for } 1 \leq x < \alpha.$$

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

$$\rho_\nu = \alpha, \quad (\nu = 1, 2, \dots, n).$$

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

$$(4.12) \quad \alpha^n = |a_n|,$$

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

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

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

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

$$(5.2) \quad |z_i| \leq \alpha, \quad (i = 1, 2, \dots, n);$$

similarly,

$$(5.3) \quad |\omega_i| \leq \alpha, \quad (i = 1, 2, \dots, k - n).$$

Therefore, by (5.2), we get

$$(5.4) \quad |a_n| = |z_1| \cdot |z_2| \cdot \dots \cdot |z_n| \leq \alpha^n.$$

The right equality sign in (5.4) cannot hold, since  $L(\alpha) \geq 3$ . 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),

$$(5.5) \quad \alpha^k - \alpha^j \leq |a_n| \alpha^{k-n}.$$

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  $k \geq n$ . Now,

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

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

$$(5.7) \quad |a_n| \alpha^k = r \alpha^n.$$

If  $k \neq n$ ,  $\alpha^{k-n} = r/|a_n|$ , contradicting the hypothesis that  $L(\alpha) \geq 3$  (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  $g/\alpha$  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  $j < k$ ,

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

by (2.1).

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

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

Dividing by  $\alpha^{n-1}$ , 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  $\alpha$ :

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

( $K > 0$ ) has  $\alpha$  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  $\alpha^t$  is rational, then  $L(\alpha) = 2$ .*

**Proof.** Let  $h$  denote the *smallest* positive integer such that  $\alpha^h$  is rational; let  $\alpha^h = v$ . Since  $\alpha$  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  $L(\alpha) \geq 3$ . Suppose that each of the pairs  $(j, k), (j', k')$  forms a binary class of  $\mathcal{S}/\alpha$  ( $j < k, j' < k'$ ). 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,

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

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  $L(\alpha) \geq 3$ , in view of Theorem 1.

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

$$(6.2) \quad k - j \leq n - \log_\alpha(\alpha^n - |a_n|).$$

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

$$(6.3) \quad k - j \leq N.$$



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

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

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,

$$(8.1) \quad \alpha^k - \alpha^j = r,$$

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

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

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  $\alpha$ .

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  $g/\alpha$  is unitary. If  $a > 0$ , it follows from Corollary 5.1 that  $g/\alpha$  is unitary. This proves part (a).

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

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

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

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

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

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

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  $\alpha^p$  is of type*

$$(10.4) \quad \alpha^p = c\alpha^{n-q} + c\alpha^{n-2q} + c\alpha^{n-3q} + \dots + c\alpha^{n-mq},$$

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

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

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

$$(10.5) \quad \alpha^p = c_q\alpha^{n-q} + c_{q+1}\alpha^{n-q-1} + c_{q+2}\alpha^{n-q-2} + \dots + c_{n-1}\alpha + c_n,$$

all  $c_i \geq 0, c_q > 0, q \geq 1$ . 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  $\alpha^{p+1}, \alpha^{p+2}, \dots, \alpha^{p+q-1}$  will each have canonical forms of degree *higher* than  $(n - q)$ , so that none of the integers  $p + 1, p + 2, \dots, p + q - 1$  can belong to  $C_0$ . Moreover, since  $\alpha^{p+q}$  will contain the "constant" term  $c_q K$  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  $\alpha^w$  ( $w$  integral), we shall mean the canonical form of  $\alpha^w$  with all zero terms omitted. We note that the pure-canonical form of  $\alpha^w$  ( $w \geq 0$ ) 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  $\alpha^p$  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,  $\alpha^{p+q}$  would contain the exponent  $(u+q)$  in its pure-canonical form, while  $\alpha^p$  does not, which is impossible.

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

$$(10.6) \quad \alpha^p = c_q \alpha^{n-q} + c_{2q} \alpha^{n-2q} + \dots + c_{mq} \alpha^{n-mq} + \dots + c_{vq} \alpha^{n-vq},$$

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

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

$$(10.7) \quad \alpha^p = c_q \alpha^{n-q} + c_{2q} \alpha^{n-2q} + \dots + c_{mq} \alpha^{n-mq},$$

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

$$(10.8) \quad \alpha^{p+q} = c_{2q} \alpha^{n-q} + c_{3q} \alpha^{n-2q} + \dots + c_{mq} \alpha^{n-(m-1)q} + c_q \alpha^{n-mq} + c_q K.$$

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

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

completing the proof of Lemma 10.1.

It will now be shown that if there exists an integer  $p$  such that  $\alpha^p$  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  $\alpha^p$  is of form (10.4), then  $K=1$  in (10.1), and  $c=1$  in (10.4).*

**Proof.** Dividing (10.4) by  $\alpha^{n-mq}$ , we have

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

Therefore,

$$(10.10) \quad x^{p-n+mq} - c[x^{(m-1)q} + x^{(m-2)q} + \dots + x^q + 1] = (x^n - x^{n-r} - K) \cdot P(x),$$

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

$\alpha^{p-n+mq}$  is also a unit. But, according to (10.9),  $c$  must divide  $\alpha^{p-n+mq}$  (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  $\alpha^p$  has a canonical form of type (10.4), then  $n < p < n+r$ .*

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

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

$$(10.11) \quad \alpha^n = \alpha^{n-r} + 1.$$

Therefore,

$$(10.12) \quad \alpha^{n+r} = \alpha^{n-r} + \alpha^r + 1.$$

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

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

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

Thus, the canonical form of  $\alpha^p$  will have at least one coefficient  $\geq 2$ , since  $\alpha^p = \alpha^{p-2n} \cdot \alpha^{2n}$  and all coefficients in the canonical form of  $\alpha^{p-2n}$  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  $\alpha^p$  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

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

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

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

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

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

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

12. **Some unanswered questions.** The decomposition  $\mathcal{G}/\alpha$  has at most a finite number of binary classes, by Theorem 3. However, the authors have no example of an  $\alpha$  for which  $\mathcal{G}/\alpha$  has *more than two* binary classes; nor do they have an example for which  $\mathcal{G}/\alpha$  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  $\alpha$  for which  $\mathcal{G}/\alpha$  has *more than two* binary classes?
- (2) Does there exist an  $\alpha$ , other than the case where  $M_\alpha(x)$  is of the form  $x^{3t}-x^t-1$ , for which  $\mathcal{G}/\alpha$  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  $\alpha$  of  $Q(x)$  will induce a decomposition  $\mathcal{G}/\alpha$  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,  $\mathcal{G}/\alpha$  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 algebraischen 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 reducible 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