The conditions of the theorem are necessary by the results of §3 and the corollary of §8. We may show that the conditions are sufficient by an argument following closely that used in proving the sufficiency of the condition in §6.

The first example of §7 shows that the conditions of the theorem are not sufficient if we do not specify that M is locally connected.

THE UNIVERSITY OF MICHIGAN

ON THE GENERALIZATION OF TRIGONOMETRIC IDENTITIES IN ARITHMETICAL PARAPHRASING*

BY H. T. ENGSTROM†

1. *Introduction.* Identities of the type

$$\sum_{s=1}^{m}\alpha_s \sin a_s x \equiv \sum_{t=1}^{n}\beta_t \sin b_t x, \tag{1}$$

where α_s, a_s, β_t, b_t are rational integers, arise in the comparison of like powers of the modulus when an elliptic function is represented in more than one way by trigonometric series. The following theorem is used in obtaining arithmetical results from such identities.

THEOREM 1. *If $g(x)$ is an arbitrary, single-valued, odd function, defined for $x=a_s$, $s=1, 2, \cdots, m$, and $x=b_t$, $t=1, 2, \cdots, n$, then* (1) *implies*

$$\sum_{s=1}^{m}\alpha_s g(a_s) = \sum_{t=1}^{n}\beta_t g(b_t). \tag{2}$$

Similarly, for cosines, we have the following statement.

THEOREM 2. *If $f(x)$ is an arbitrary, single-valued, even function, defined for $x=a_s$, $s=1, 2, \cdots, m$, and $x=b_t$, $t=1, 2, \cdots, n$, then*

$$\sum_{s=1}^{m}\alpha_s \cos a_s x \equiv \sum_{t=1}^{n}\beta_t \cos b_t x \tag{3}$$

---

* Presented to the Society, April 5, 1930.

† National Research Fellow, California Institute of Technology.

implies

$$\sum_{s=1}^{m}\alpha_s f(a_s) = \sum_{t=1}^{n}\beta_t f(b_t). \tag{4}$$

The method of proof for these theorems suggested by Liouville* assumes that the functions may be represented by a Fourier series. Nazimoff† also makes use of the Fourier series property. The method is perfectly general since the functions $f(x)$ and $g(x)$ are defined for only a finite number of values of the argument and hence by interpolation we may represent them by a Fourier series. It is desirable, however, to give a purely algebraic proof of the replacement principle. E. T. Bell,‡ in his fundamental paper on arithmetical paraphrases, avoids the Fourier series by making use of the lemmas which follow.

LEMMA 1. *If the a_s are rational integers $\gtreqless 0$ and the b_t rational integers $\gtrless 0$, and if for all integral values >0 of k*

$$\sum_{s=1}^{m}a_s^{2k} = \sum_{t=1}^{n}b_t^{2k},$$

then (i) *$m \geqq n$ and precisely $(m-n)$ of the $a_s = 0$;* (ii) *if, without loss of generality, the n non-zero a_s are $a_1, a_2, \cdots, a_n$, then the $a_1^2, a_2^2, \cdots, a_n^2$ are a permutation of the $b_1^2, b_2^2, \cdots, b_n^2$.*

LEMMA 2. *If the a_s, b_t are integers >0, and if there is an infinity of odd integers $k>0$, for which*

$$\sum_{s=1}^{m}a_s^k = \sum_{t=1}^{n}b_t^k,$$

then $m=n$, and the a_s are a permutation of the b_t.

Bell (loc. cit.) has given a simple algebraic proof of Lemma 1. Lemma 2, however, has not been proved by purely algebraic means. The proofs given by E. Swift§ and C. F. Gummer‖ depend on continuity considerations. In the following paper

* *Note de M. Liouville*, Journal de Mathématiques, vol. 7 (1862), p. 48.

† Nazimoff, Annales Scientifiques de l'École Normale, vol. 3 (1868), p. 149.

‡ Bell, Transactions of this Society, vol. 22 (1921), p. 17.

§ E. Swift, American Mathematical Monthly, vol. 24 (1917), p. 288.

‖ C. F. Gummer, Transactions of this Society, vol. 23 (1922), p. 280.

the author presents a direct algebraic proof of Theorems 1 and 2 based on the irreducibility of the cyclotomic equation.

2. *Cyclotomic Fields.* Consider the cyclotomic field K of degree $p-1$ defined by a root of the equation

$$\phi(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = 0, \tag{5}$$

where p is an odd prime. From the irreducibility of $\phi(x)$ the following theorem is obvious.

THEOREM 3. *The algebraic integers*

$$e^{2k\pi i/p},\ k = \pm 1,\ \pm 2, \cdots, \pm \frac{p-1}{2}, \tag{6}$$

are linearly independent for rational coefficients.

We shall now consider Theorem 1. Let us choose an odd prime p such that

$$\frac{p-1}{2} > \max(m, n, |a_s|, |b_t|). \tag{7}$$

Substituting $x = 2\pi/p$ in (1) and replacing the sines by exponentials we obtain

$$\sum_{s,t}\left\{\alpha_s e^{2\pi a_s i/p} - \alpha_s e^{-2\pi a_s i/p} - \beta_t e^{2\pi b_t i/p} + \beta_t e^{-2\pi b_t i/p}\right\} = 0. \tag{8}$$

From (7), the terms in (8) are either zero or belong to the set (6). Hence the coefficient of $e^{2\pi ki/p}$, $k = \pm 1, \pm 2, \cdots, \pm (p-1)/2$ in (8) must vanish. Let us consider the three cases: (i) the a_s and b_t all different from zero and of like sign; (ii) some a_s or b_t equal to zero and the remainder of like sign; (iii) the general case.

In case (i) it is seen that the coefficient of sin kx, $k = \pm 1$, $\pm 2, \cdots, \pm (p-1)/2$, in (1) is precisely that of $e^{2\pi ki/p}$ in (8) and hence must vanish. The following generalization of Theorem 1 follows immediately.

THEOREM 4. *If a_s and b_t satisfy* (i) *and $F(x)$ is an arbitrary function defined for $x = a_s$ and $x = b_t$, then* (1) *implies*

$$\sum_{s=1}^{m}\alpha_s F(a_s) = \sum_{t=1}^{n}\beta_t F(b_t).$$

We now turn to case (ii). Let $F_0(x)$ be any function for which $F_0(0)=0$. We substitute $F_0(a_s)$ and $F_0(b_t)$ respectively in place of $\sin(a_s x)$ and $\sin(b_t x)$ in (1). If $k \neq 0$, the coefficient of $F_0(k)$ will be precisely that of $e^{2\pi ki/p}$ in (8) and hence vanishes. If $k=0$, by definition $F_0(k)=0$, and hence we have the following theorem.

THEOREM 5. *If a_s, b_t satisfy* (ii) *and $F_0(x)$ is an arbitrary function defined for $x=a_s$ and $x=b_t$ and vanishing for $x=0$, then* (1) *implies*

$$\sum_{s=1}^{m} \alpha_s F_0(a_s) = \sum_{t=1}^{n} \beta_t F_0(b_t).$$

Let us consider the general case (iii) and let $g(x)$ be an arbitrary odd function. If a_s is positive we replace $\sin(a_s x)$ in (1) by $g(a_s)$, if negative by $-g(-a_s)$. Similarly for b_t. The resulting coefficient of $g(k)$, $k=1, 2, \cdots, (p-1)/2$, is seen to be precisely that of $e^{2\pi ki/p}$ in (8) and hence is zero. Since $x=0$ implies $g(x)=0$ and $g(x)=-g(-x)$, Theorem 1 follows.

Let us consider Theorem 2. We again choose p in accordance with (7). Substituting $x=2\pi/p$ in (3) and expressing in terms of exponentials we obtain

$$(9) \quad \sum_{s,t} \left\{ \alpha_s e^{2\pi a_s i/p} + \alpha_s e^{-2\pi a_s i/p} - \beta_t e^{2\pi b_t i/p} - \beta_t e^{-2\pi b_t i/p} \right\} = 0.$$

The reasoning used for Theorem 1 must be modified slightly on account of the rational terms which may enter for vanishing a_s or b_t. Since (6) are the roots of (5) we have

$$\sum_{k=\pm 1, \pm 2, \cdots, \pm (p-1)/2} e^{2\pi ki/p} = -1.$$

Furthermore, from Theorem 3, this representation of -1 as a rational linear combination of (6) is unique. Hence we have the following theorem.

THEOREM 6. *If c_k and R are rational, then*

$$\sum_{k=\pm 1, \pm 2, \cdots, \pm (p-1)/2} c_k e^{2\pi ki/p} = R$$

implies $c_k = -R$, $k = \pm 1, \pm 2, \cdots, \pm (p-1)/2$.

It follows from this theorem and (7) that the coefficients of $e^{2\pi ki/p}$ in (9) and also the rational term must vanish. Let us now consider two cases: (i) a_s and b_t all of like sign or zero; and

(ii) the general case. In case (i) let $F(x)$ be an arbitrary function defined for $x=a_s$ and $x=b_t$. We substitute $F(a_s)$ and $F(b_t)$ for $\cos(a_s x)$ and $\cos(b_t x)$ respectively. The coefficient of $F(l)$, $l=0, 1, 2, \cdots, (p-1)/2$, will be precisely that of $e^{2\pi li/p}$ in (9) and hence vanishes. Hence we have the following theorem:

THEOREM 7. *If the a_s, b_t in* (3) *satisfy* (i) *and $F(x)$ is an arbitrary function defined for $x=a_s$ and $x=b_t$, then* (3) *implies*

$$\sum_{s=1}^{m}\alpha_s F(a_s) = \sum_{t=1}^{n}\beta_t F(b_t).$$

For the general case (ii), let $f(x)$ be an arbitrary even function. If a_s is positive, substitute $f(a_s)$ in place of $\cos(a_s x)$ in (3), if negative, substitute $f(-a_s)$. Similarly for b_t. Then, as above, the coefficient of $f(l)$, $l=0, 1, 2, \cdots, (p-1)/2$, will be precisely that of $e^{2\pi li/p}$ in (9) and hence vanishes. Theorem 2 follows immediately.

3. *Removal of Conditions.* The condition that α_s, a_s, β_t, b_t be rational integers may be easily lessened. If a_s and b_t are of the form $A_s N$ and $B_t N$ respectively, where A_s and B_t are rational and N is any real number, the transformation $x=MNy$, where M is a common multiple of the denominators of A_s and B_t, reduces the problem to the cases already considered. The theorems may also be generalized to algebraic α_s and β_t. We may suppose them algebraic integers since denominators may be eliminated by cross-multiplication and we may suppose that they all belong to an algebraic field K_1 of degree r. We shall show that p may be chosen so that (5) is irreducible in K_1.

By writing

$$\phi(x) = \prod_{k=\pm 1,\pm 2,\cdots,\pm(p-1)/2} (x - e^{2\pi ki/p})$$

it is seen that $\phi(x)$ may be reducible only in those fields which are subfields of K. We first place on p the condition

$$\left(\frac{p-1}{2}, r\right) = 1 \tag{10}$$

which insures that r and $p-1$ have at most the common divisor 2, that is, K and K_1 have at most a quadratic subfield in common. But the field K_1 contains only a finite number of distinct

quadratic subfields. Suppose that these fields are generated by $c_1^{1/2}, c_2^{1/2}, \cdots, c_\mu^{1/2}$. Since the only quadratic field in which $\phi(x)$ is reducible is that generated by

$$[(-1)^{(p-1)/2} \cdot p]^{1/2},$$

if we impose on p the further condition

$$(p, c_1, c_2, \cdots, c_\mu) = 1, \tag{11}$$

it follows that K and K_1 will have no common subfield and hence $\phi(x)$ will be irreducible in K_1. Hence a linear combination of (6) with coefficients in K_1 is zero if, and only if, each coefficient is zero. Theorems 1, 4, and 5 generalize directly. Theorem 6 takes the following form.

THEOREM 8. *If p satisfies* (10) *and* (11), *the relation*

$$\sum_k \theta_k e^{2\pi ki/p} = \rho,$$

where θ_k and ρ belong to K_1, implies $\theta_k = -\rho$, $k = \pm 1, \pm 2, \cdots, \pm(p-1)/2$.

Theorems 1 and 7 generalize immediately.

To extend the theorems to arbitrary complex α_s, β_t let us suppose that some of them are not algebraic. We may then replace the α_s, β_t by linear combinations of a set $1, \pi_1, \pi_2, \cdots, \pi_\nu$ with algebraic coefficients, where $1, \pi_1, \pi_2, \cdots, \pi_\nu$ are linearly independent for algebraic coefficients. Hence, for similar choice of p, (8) and (9) imply $\nu+1$ equations of the same type with algebraic coefficients and the theorems follow. The results are combined in the following theorem.

THEOREM 9. *The theorems of this paper are valid for arbitrary complex α_s, β_t and for a_s, b_t of the form $A_sN, B_t N$ respectively, where A_s, B_t are rational and N is an arbitrary complex number.*

CALIFORNIA INSTITUTE OF TECHNOLOGY