PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 81, Number 2, February 1981

# GENERALIZED CYCLOTOMIC PERIODS

RONALD J. EVANS

ABSTRACT. Let $n$ and $q$ be relatively prime integers with $n > 1$, and set $N$ equal to twice the product of the distinct prime factors of $n$. Let $t(n)$ denote the order of $q$ (mod $n$). Write $\eta = \sum_{v=0}^{t(n)-1} a_v \zeta_n^{q^v}$, where $\zeta_n = \exp(2\pi i/n)$. If $a_v = 1$ for all $v$, then $\eta$ is Kummer's cyclotomic period, and if $a_v = \exp(2\pi i v/t(n))$ for each $v$, then $\eta$ is a type of Lagrange resolvent. For certain classes of $a_v \in Q(\zeta_n^N)$, necessary and sufficient conditions for the vanishing of $\eta$ are given, and the degree of $\eta$ over Q is determined.

**1. Introduction and notation.** Let $n$ and $q$ be fixed relatively prime integers with $n > 1$, and set $N$ equal to twice the product of the distinct prime factors of $n$. Fix an integer $s$ prime to $n$ and set $K_n = K_{n,s} = Q(\zeta_s, \zeta_n^N)$, where $\zeta_n = \exp(2\pi i/n)$. For any integer $j$ prime to $n$, define $\sigma_j \in \mathrm{Gal}(Q(\zeta_{ns})/Q(\zeta_s))$ by $\sigma_j(\zeta_n) = \zeta_n^j$. Let $t(n)$ denote the order of $q$ (mod $n$). Fix $a_v \in K_n$ $(0 \leq v < t(n))$ with not all $a_v$ vanishing, and define the *generalized cyclotomic period* $\eta$ by

$$\eta = \sum_{v=0}^{t(n)-1} a_v \zeta_n^{q^v}.$$

If all $a_v$ equal 1, then $\eta$ is the cyclotomic period $\sum \zeta_n^{q^v}$ first studied for general $n$ by Kummer [2], but studied for prime $n$ over half a century earlier by Gauss. If $a_v = \exp(2\pi i v/t(n))$ for each $v$, where $n$ is a prime power, then $\eta$ is a type of Lagrange resolvent studied in Weber's book [5, §19].

Fuchs [1] proved in essence the following facts about cyclotomic periods.

(1) If $t(n) = pt(n/p)$ for some prime $p$ dividing $n$, then $\sum \zeta_n^{q^v} = 0$; and, conversely,

(2) if $\sum \zeta_n^{q^v} = 0$, then $t(n) = pt(n/p)$ for some prime $p$ dividing $n$; and

(3) if $\sum \zeta_n^{q^v} \neq 0$, then $\sum \zeta_n^{q^v}$ has degree $\phi(n)/t(n)$ over Q, where $\phi$ is Euler's function. (Earlier, Kummer [2, p. 5] had stated (3) without proof.)

We prove here some analogues of Fuchs' results, for certain generalized periods $\eta = \sum a_v \zeta_n^{q^v}$ in place of $\sum \zeta_n^{q^v}$. In the process, we obtain simple new proofs of (1), (2), and (3).

In 1977, Kurt Mahler wanted to know when the period $\sum \zeta_n^{2^v}$ vanishes, in order to glean information about the behavior of the function $\sum_{v=0}^{\infty} z^{2^v}$ near the unit circle (see [4]). Seeking to answer his query, D. H. and E. Lehmer were led to rediscover (1) and (2) (see [3], but note that the formulation given there is not quite correct).

---

Received by the editors February 14, 1980 and, in revised form, April 3, 1980. Presented at the Western Number Theory Conference, Asilomar, December 20, 1979.

*AMS (MOS) subject classifications* (1970). Primary 10G05.

*Key words and phrases*. Cyclotomic periods.

From here on, write $n = p^\alpha m$, where $p$ is prime, $p \nmid m$, and $\alpha \geqslant 1$.

## 2. Generalization of (1).

THEOREM 1. *Assume that* $a_v = \sigma_{q^v}(a_0)$ *for each* $v$, *and suppose that* $t(n) = pt(n/p)$ *for some* $p$ *dividing* $n$. *Then* $\eta = 0$.

PROOF. Let $w = t(n/p)$. We have

$$\eta = \sum_{v=0}^{t(n)-1} \sigma_{q^v}(a_0)\zeta_n^{q^v} = \sum_{u=0}^{w-1} \sigma_{q^u}\left\{ \sum_{x=0}^{p-1} \sigma_{q^{wx}}(a_0\zeta_n) \right\}.$$

Now, $q^w = 1 + jn/p$ for some $j$ prime to $p$. Since $q^{wp} \equiv 1 \pmod{n}$, we see that $p$ divides $n/p$, so $q^{wx} \equiv 1 + xjn/p \pmod{n}$ for $0 \leqslant x < p$. Thus, since $a_0 \in K_n$, $\sigma_{q^{wx}}(a_0) = a_0$. Therefore

$$\eta = \sum_{u=0}^{w-1} \sigma_{q^u}\left\{ a_0\zeta_n \sum_{x=0}^{p-1} \zeta_p^{xj} \right\} = 0,$$

since the inner sum vanishes. Q.E.D.

THEOREM 2. *Assume that* $a_v = \varepsilon^v$ *for each* $v$, *where* $\varepsilon$ *is a* $t(n)$*th root of unity. Suppose that* $t(n) = pw$ *for some prime* $p$ *dividing* $n$, *where* $w = t(n/p)$. *Write* $\varepsilon^w = \zeta_p^k$ *and* $q^w = 1 + jn/p$. *Suppose further that* $-k/j \pmod{p}$ *is not congruent to a power of* $q \pmod{p}$ (*this holds, for example, if* $\varepsilon^w = 1$). *Then* $\eta = 0$.

PROOF. The argument is essentially the same as that for Theorem 1. Q.E.D.

Theorem 2 proves one direction of Weber's theorem [5, §19] while Lemma 5 (below) proves the other direction

Note that if $a_0 = \varepsilon = 1$, then Theorems 1 and 2 reduce to (1).

## 3. Generalization of (2).

LEMMA 3. *We have* $t(n) \neq pt(n/p)$ *if and only if either* $t(n) = t(mp)$ *or*

$$p^\alpha = 2^\alpha \geqslant 8, \quad t(n) = 2t(m), \quad 2 \nmid t(m), \quad \text{and} \quad q \equiv 3 \pmod{4}. \tag{4}$$

PROOF. If $t(n) = t(mp)$ or (4) holds, clearly $t(n) \neq pt(n/p)$. Conversely, suppose that $t(n) \neq pt(n/p)$ and $t(n) \neq t(mp)$. We must prove (4). Note that $p^A \| (q^{t(mp)}-1)$ for some $A$ with $1 \leqslant A < \alpha$. Suppose that $p$ is odd. Then $p^{A+B} \| (q^{p^B t(mp)}-1)$ for each $B \geqslant 0$. Thus $t(mp^{A+B}) = p^B t(mp)$ for each $B \geqslant 0$. Therefore, $t(n) = pt(n/p)$, a contradiction. Thus $p = 2$. We can now obtain a contradiction exactly as before, unless $A = 1$ and $t(n) = 2t(2m)$. These last equalities are easily seen to imply (4). Q.E.D.

LEMMA 4. *Suppose that* $p$ *is the largest prime factor of* $n$, *and* $t(p^\alpha) = pt(p^{\alpha-1})$. *Then* $t(n) = pt(n/p)$.

PROOF. If $n = p^\alpha$, the result is obvious, so we may assume that $p$ is odd. Assume that $t(n) = t(mp)$. Then $t(p^\alpha) | t(mp)$, so by hypothesis, $p | t(mp)$. Thus $p | \phi(mp)$, a contradiction. Therefore $t(n) \neq t(mp)$. Since also $p$ is odd, the result follows from Lemma 3. Q.E.D.

LEMMA 5. *Suppose that* $n = p^\alpha$ *and* $\eta = 0$. *Then* $t(n) = pt(n/p)$.

PROOF. Assume that $t(n) \neq pt(n/p)$. Then by Lemma 3, either $t(n) = t(p)$ or $8|n$, $t(n) = 2$, $q \equiv 3 \pmod 4$. In the latter event, $0 = \eta = a_0\zeta_n + a_1\zeta_n^q$, so $\zeta_n^{q-1} \in K_n$, which is impossible because $2\|(q-1)$. Thus $t(n) = t(p)$. Since $\eta = 0$, $t(n) > 1$. Thus $p > 2$. Let $r_v$ denote the least positive residue of $q^v \pmod p$. Then

$$0 = \eta = \sum_{v=0}^{t(p)-1} \left(a_v\zeta_n^{q^v - r_v}\right)\zeta_n^{r_v}$$

and the expressions in parentheses are in $K_n$. Since the elements $\zeta_n^{r_v}$ $(0 \leqslant v < t(p))$ are distinct elements of a basis for $K_n(\zeta_n)$ over $K_n$, it follows that all $a_v$ vanish, a contradiction. Q.E.D.

LEMMA 6. *Write $z = t(p^\alpha)$, $Q = q^z$, and let $T(m)$ denote the order of $Q \pmod m$. Then*

$$\sigma_{m+p^\alpha}(\eta) = \sum_{u=0}^{z-1} \sigma_{q^u}(\delta_u)\zeta_{p^\alpha}^{q^u}, \tag{5}$$

*where*

$$\delta_u = \sum_{x=0}^{T(m)-1} \theta_{x,u}\zeta_m^{Q^x}, \tag{6}$$

$$\theta_{x,u} = \sigma_{m+p^\alpha}\sigma_{q^u}^{-1}(a_{zx+u}). \tag{7}$$

PROOF. Since $T(m) = t(n)/z$ and $\zeta_{p^\alpha}^Q = \zeta_{p^\alpha}$,

$$\sigma_{m+p^\alpha}(\eta) = \sum_{v=0}^{t(n)-1} \sigma_{m+p^\alpha}(a_v)\zeta_m^{q^v}\zeta_{p^\alpha}^{q^v} = \sum_{u=0}^{z-1}\sum_{x=0}^{T(m)-1} \sigma_{m+p^\alpha}(a_{zx+u})\zeta_m^{Q^x q^u}\zeta_{p^\alpha}^{q^u},$$

and the result follows. Q.E.D.

THEOREM 7. *Suppose that $\eta = 0$. Then $t(n) = pt(n/p)$ for some $p$ dividing $n$.*

PROOF. The notation of Lemma 6 will be used here. We induct on the number of distinct prime factors of $n$. The induction starts by Lemma 5, so it can be assumed that $n$ is not a prime power. Let $p$ be the largest prime factor of $n$. First suppose that $\delta_u \neq 0$ for some $u$. By (6) and (7), $\sigma_{q^u}(\delta_u) \in K_{p^\alpha, ms}$. Since the left side of (5) vanishes, we may apply Lemma 5 to the generalized period on the right side of (5) to conclude that $t(p^\alpha) = pt(p^{\alpha-1})$. Thus $t(n) = pt(n/p)$ by Lemma 4. Finally, suppose that $\delta_u = 0$ for each $u$. Fix $u$ such that $\theta_{x,u} \neq 0$ some for $x$ (this is possible by (7)). All of the $\theta_{x,u}$ are in $K_{m,sp^\alpha}$, so by (6) and the induction hypothesis, $T(m) = rT(m/r)$ for some prime $r$ dividing $m$. Multiplying by $t(p^\alpha)$, we find that $t(n) = rt(n/r)$. Q.E.D.

REMARK. If $n = mp^\alpha$ with $\alpha > 1$ and $L = \mathbf{Q}(\zeta_{ns}^p)$, then $\eta = 0$ if and only if $\eta \in L$. Assume for the purpose of contradiction that $0 \neq \eta \in L$. By (5), $\zeta_{p^\alpha}$ is a zero of a polynomial $f(x) \in L[x]$ with $f(0) \neq 0$ but with all of $f$'s nonconstant monomials possessing the form $bx^r$, where $b \in L$, $p \nmid r$. Since $g(x) = x^p - \zeta_{p^{\alpha-1}}$ is the minimal polynomial of $\zeta_{p^\alpha}$ over $L$, $g(x)h(x) = f(x)$ for some $h(x) \in L[x]$. Since $h(0) \neq 0$, this implies that $f(x)$ has a monomial of the form $bx^r$ with $p|r$, a contradiction.

## 4. Generalization of (3).

THEOREM 8. *Suppose that* $a_v = \sigma_{q^v}(a_0)$ *for all* $v$. *If* $\eta \neq 0$, *then* $\eta$ *has degree* $\phi(n)/t(n)$ *over* $\mathbf{Q}(\zeta_s)$.

PROOF. It suffices to show that if $0 \neq \eta = \sigma_c(\eta)$, then $c \equiv$ power of $q \pmod{n}$. We will prove this by induction on the number of distinct prime factors of $n$.

Suppose that $0 \neq \eta = \sigma_c(\eta)$. By Theorem 1, $t(n) \neq pt(n/p)$, for each prime $p$ dividing $n$. Let $p$ now denote the largest prime factor of $n$. By Lemma 4, $t(p^\alpha) \neq pt(p^{\alpha-1})$, so by Lemma 3 (with $p^\alpha$ in place of $n$), either

$$t(p^\alpha) = t(p) \tag{8}$$

or

$$n = p^\alpha = 2^\alpha \geqslant 8, \quad t(2^\alpha) = 2, \quad q \equiv 3 \pmod{4}. \tag{9}$$

Suppose first that (9) holds. Then $a_0\zeta_n + a_1\zeta_n^q = \sigma_c(a_0)\zeta_n^c + \sigma_c(a_1)\zeta_n^{cq}$, so

$$\{a_0 - \sigma_c(a_0)\zeta_n^{c-1}\} = \zeta_n^{q-1}\{\sigma_c(a_1)\zeta_n^{q(c-1)} - a_1\}. \tag{10}$$

We may assume without loss of generality that $c \equiv 1 \pmod{4}$, otherwise $c$ can be replaced by $cq$. Thus, the braced expressions in (10) are in $K_n$, and since $\zeta_n^{q-1} \notin K_n$ by (9), it follows that the left side of (10) vanishes. Thus

$$\sigma_c(a_0) = a_0\zeta_n^{1-c}, \tag{11}$$

and by repeated applications of $\sigma_c$ to (11), we obtain

$$\sigma_{c^e}(a_0) = a_0\zeta_n^{1-c^e} \qquad (e \geqslant 0). \tag{12}$$

If $c = 1$, the result follows, so assume that $c \neq 1$. Then $2^B \| (c-1)$ for some $B \geqslant 2$. Assume for the purpose of contradiction that $B < \alpha$. For each $A \geqslant 0$,

$$2^{B+A} \| (c^{2^A} - 1). \tag{13}$$

Let $A = \alpha - 1 - B$. Then by (13) and (12) with $e = 2^A$, we obtain $a_0 = -a_0$, which contradicts the fact that $\eta \neq 0$. Thus $B \geqslant \alpha$, which yields the desired result.

Now suppose that (8) holds. Say $p = 2$. Then the equality $\eta = \sigma_c(\eta)$ becomes $a_0\zeta_n = \sigma_c(a_0)\zeta_n^c$. Thus (11) holds and $c \equiv 1 \pmod{4}$, so that the desired result follows as above. It remains to consider the case $p > 2$.

By (8), the right side of (5) is

$$R = \sum_{u=0}^{t(p)-1} \sigma_{q^u}(\delta)\zeta_{p^\alpha}^{q^u},$$

where

$$\delta = \sum_{x=0}^{T(m)-1} \sigma_{Q^x}(b_0)\zeta_m^{Q^x}, \qquad b_0 = \sigma_{m+p^\alpha}(a_0).$$

Since $0 \neq \eta = \sigma_c(\eta)$, it follows from (5) that $0 \neq R = \sigma_c(R)$ (and in particular, $\delta \neq 0$). For $0 \leqslant u < t(p)$, write

$$q^u = ps_u + r_u, \quad cq^u = ps'_u + r'_u \qquad (0 < r_u, r'_u < p). \tag{14}$$

Clearly the $r_u$ are distinct and the $r'_u$ are distinct.

We have

$$\sum_{u=0}^{t(p)-1} \left(\sigma_{q^u}(\delta)\zeta_{p^{\alpha-1}}^{s_u}\right)\zeta_{p^\alpha}^{r_u} = R = \sigma_c(R) = \sum_{u=0}^{t(p)-1} \left(\sigma_{cq^u}(\delta)\zeta_{p^{\alpha-1}}^{s'_u}\right)\zeta_{p^\alpha}^{r'_u} \quad .$$

Since the elements $\zeta_{p^\alpha}^1, \ldots, \zeta_{p^\alpha}^{p-1}$ are linearly independent over $\mathbf{Q}(\zeta_{ns}^p)$, there exists a fixed value of $u$ such that

$$r'_u = r_0 = 1 \tag{15}$$

and

$$\delta = \delta\zeta_{p^{\alpha-1}}^{s_0} = \sigma_{cq^u}(\delta)\zeta_{p^{\alpha-1}}^{s'_u}.$$

Thus, by (14) and (15),

$$d = cq^u = 1 - py \tag{16}$$

and

$$\sigma_d(\delta) = \delta\zeta_{p^{\alpha-1}}^{y}, \tag{17}$$

where $y = -s'_u$. If $d = 1$, the result follows, so assume that $d \neq 1$. Repeated applications of $\sigma_d$ to (17) yield

$$\sigma_{d^e}(\delta) = \delta\zeta_{p^{\alpha-1}}^{y(d^e-1)/(d-1)} \qquad (e \geqslant 0). \tag{18}$$

We have $p^B \| (d - 1)$ for some $B \geqslant 1$. Thus, by (16),

$$p^{B-1} \| y. \tag{19}$$

Assume for the purpose of contradiction that $B < \alpha$. For each $A \geqslant 0$,

$$p^{A+B} \| (d^{p^A} - 1). \tag{20}$$

Let $A = \alpha - 1 - B$. By (20) and (18) with $e = p^A$, $p^{\alpha-1} | y(d^{p^A} - 1)/(d - 1)$, so by (19), $p^\alpha | (d^{p^A} - 1)$, which contradicts (20). Thus $B \geqslant \alpha$, so

$$d \equiv 1 \pmod{p^\alpha}. \tag{21}$$

This completes the proof if $n$ is a prime power, i.e., if $m = 1$. Thus assume that $m > 1$. By (19), $p^{\alpha-1} | y$, so by (17),

$$\sigma_d(\delta) = \delta. \tag{22}$$

Since $\delta$ equals the generalized period $\sum_{x=0}^{T(m)-1} \sigma_{Q^x}(b_0)\zeta_m^{Q^x}$ with $0 \neq b_0 \in K_{m,sp^\alpha}$ and $\sigma_{Q^x} \in \mathrm{Gal}(\mathbf{Q}(\zeta_{msp^\alpha})/\mathbf{Q}(\zeta_{sp^\alpha}))$, it follows from (21), (22), and the induction hypothesis that $d \equiv Q^h \pmod{m}$ for some $h$. Since $Q \equiv 1 \pmod{p^\alpha}$, (21) yields $d \equiv Q^h \pmod{p^\alpha}$. Thus $d \equiv Q^h \pmod{n}$ and $c \equiv$ power of $q \pmod{n}$. Q.E.D.

Theorem 8 states that if $L$ is a field with $\mathbf{Q}(\zeta_{sn}) \supset L \supset \mathbf{Q}(\zeta_s)$ such that $\mathbf{Q}(\zeta_{sn})$ is cyclic over $L$, then the degree of $\mathrm{Tr}(a_0\zeta_n)$ over $\mathbf{Q}(\zeta_s)$ is either 0 or $|L\colon \mathbf{Q}(\zeta_s)|$, where Tr denotes the trace map from $\mathbf{Q}(\zeta_{sn})$ to $L$. In other words, if $\mathrm{Tr}(a_0\zeta_n)$ is nonzero, then it has the maximum possible degree over $\mathbf{Q}(\zeta_s)$ that any element of $L$ can have. A modification of the proof of Theorem 8 shows that the hypothesis that $\mathbf{Q}(\zeta_{sn})/L$ is cyclic may be dropped.

The author is very grateful to the Lehmers for their encouragement and helpful comments.

## REFERENCES

1. L. Fuchs, *Ueber die Perioden, welche aus den Wurzeln der Gleichung* $\omega^n = 1$ *gebildet sind, wenn n eine zusammengesetzte Zahl ist*, J. Reine Angew. Math. **61** (1863), 374–386.

2. E. Kummer, *Theorie der idealen Primfaktoren der complexen Zahlen, welche aus den Wurzeln der Gleichung* $\omega^n = 1$ *gebildet sind, wenn n eine zusammengesetzte Zahl ist*, Math. Abh. Kon. Akad. Wiss. Berlin (1856), 1–47; Collected Papers, vol. 1, Springer-Verlag, Berlin and New York, 1975, pp. 583–629.

3. D. H. Lehmer and E. Lehmer, Notices Amer. Math. Soc. **25** (1978), 145.

4. K. Mahler, *On a special function*, J. Number Theory **12** (1980), 20–26.

5. H. Weber, *Lehrbuch der Algebra*, 3rd ed., vol. 2, Chelsea, New York, 1961.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA-SAN DIEGO, LA JOLLA, CALIFORNIA 92093