JOURNAL OF NUMBER THEORY 7, 108–120 (1975)

On a Theorem of Iwasawa

RAYMOND AYOUB

Department of Mathematics, Pennsylvania State University, University Park, Pennsylvania 16802

Communicated by S. Chowla

Received November 29, 1972

1. INTRODUCTION

In this section we shall give the setting which leads to a formulation of Iwasawa's Theorem [1].

Let p be a prime, $p > 3$ and let

$$t = \frac{p-1}{2}. \tag{1}$$

Chowla [2] proved that the t real numbers $\cot(2\pi l/p)$ $(l = 1, 2,..., t)$ are linearly independent over the field Q of rational numbers.

Following Iwasawa's notation, let Q_p be the p-adic completion of Q and let ν_p be the normalized valuation on Q_p such that $\nu_p(p) = 1$. For $a = 1, 2,..., p-1$, it is easily seen that

$$\alpha_a = \lim_{n\to\infty} a^{p^n} \tag{2}$$

exists in Q_p, that $\alpha_a \equiv a \pmod p$, and that α_a is a $(p-1)$-st root of unity in Q_p.

Let ζ be a primitive pth root of unity in the complex field and let $K = Q(\zeta)$; let $K_p = Q_p(\lambda)$, where K_p is the local cyclotomic field of pth roots of unity over Q_p.

Let ρ be a primitive $(p-1)$-st root of unity in the complex field. There is a natural isomorphism from $Q(\zeta, \rho)$ into K_p given by $\rho \to \alpha_g$, $\zeta \to \lambda$, where g is a primitive root mod p. Call this isomorphism η. The valuation ν_p can be extended to K_p and hence can be defined on $Q(\zeta, \rho)$ as follows: If $\beta \in Q(\zeta, \rho)$, then define

$$\nu_p(\beta) = \nu_p(\eta(\beta)). \tag{3}$$

We use the same symbol for the valuation on $Q(\zeta, \rho)$ as no confusion will arise.

Let

$$\xi_l = \frac{\zeta^l + \zeta^{-l}}{\zeta^l - \zeta^{-l}} = i \cot\left(\frac{2\pi l}{p}\right) \tag{4}$$

and let γ be the automorphism $\zeta \to \zeta^{-1}$ of $K = Q(\zeta)$. Let

$$K^+ = \{k \in K;\ \gamma(k) = k\}, \tag{5}$$

$$K^- = \{k \in K;\ \gamma(k) = -k\}. \tag{6}$$

K^- is not a subfield of K, but both K^+ and K^- are vector spaces over Q of dimension t. Since $\gamma(\xi_l) = -\xi_l$ $(l = 1, 2,..., t)$, it follows that

$$\xi_l \in K^- \ (l = 1, 2,..., t)$$

and hence, by Chowla's theorem, ξ_l form a basis for K^- over Q. Moreover $\zeta - \zeta^{-1} \in K^-$; therefore, there exist $x_l \in Q$ $(l = 1, 2,..., t)$ such that

$$\zeta - \zeta^{-1} = \sum_{l=1}^{t} x_l \xi_l \tag{7}$$

This may be rewritten as

$$2 \sin \frac{2\pi}{p} = \sum_{l=1}^{t} x_l \cot\left(\frac{2\pi}{p} l\right). \tag{8}$$

Let

$$\delta_p = \max_l \left(-\nu_p(x_l)\right). \tag{9}$$

Suppose that χ is a character mod p and consider

$$u_\chi = \frac{2\chi(2)}{p} \sum_{m=1}^{p-1} m\chi(m);$$

then $u_\chi \in Q(\zeta, \rho)$. If $\chi(-1) = 1$ and χ is nonprincipal, then $u_\chi = 0$; otherwise, if $\chi(-1) = -1$, $u_\chi \neq 0$. Let

$$e_\chi = \nu_p(u_\chi).$$

Iwasawa proved the following theorem:

$$\delta_p = \max_\chi \left(e_\chi\ ;\ \chi(-1) = -1\right). \tag{10}$$

He deduced that (i) in general $\delta_p \geqslant 0$, (ii) $\delta_p = 0$ if and only if the prime p is regular. Let $h = h_1 h_2$, where h is the class number of K and h_2 the class number of K^+.

From (10) Iwasawa derived the highly interesting fact that, if $\nu_p(h_1) = s$ while r = number of Bernouilli numbers B_n $(1 \leqslant n \leqslant (p-3)/2)$ divisible by p, then $s \geqslant r$ and $s = r$ if and only if $\delta_p \leqslant 1$.

The object of this note is to give an "explicit" evaluation of the numbers x_l and to deduce (10) as a consequence. In the course of the derivation, an alternate proof of Chowla's theorem will appear.

2. Evaluation of x_l

We shall first state the result and later give an indication of how it was arrived at and incidentally give another proof of Chowla's Theorem.

THEOREM 2.1. *Let χ be a character* mod p *such that* $\chi(-1) = -1$, *and let*

$$S(\chi) = \sum_{m=1}^{p-1} m\chi(m); \tag{11}$$

then

$$x_l = \frac{2p}{p-1} \sum_{\chi} \frac{\bar{\chi}(2l)}{S(\chi)}, \qquad l = 1, 2, \ldots, t \tag{12}$$

and the summation is over all characters χ such that $\chi(-1) = -1$. There are t of these.

Proof. We first remark that the right-hand side is meaningful since $S(\chi)$, being a factor of the first factor of h, is different from 0. Secondly, $x_l \in Q$. This fact will emerge in Section 3 but to make Section 2 independent of Section 3, we give a proof.

Let g be a primitive root mod p and choose χ_0 so that $\chi_0(g) = \rho^{-1}$, where ρ is a primitive $(p-1)$-st root of unity. χ_0 generates the cyclic group of characters. The characters for which $\chi(-1) = -1$ are determined then by $-1 = \chi_0^m(-1) = \chi_0^m(g^t) = \rho^{-mt}$. It follows that m must be odd. The automorphisms of $Q(\rho)$ are given by $\mu_a : \rho \to \rho^a$ with $(a, p-1) = 1$. Thus, if $2l \equiv g^b (\mathrm{mod}\, p)$, then

$$\chi(2l)\, S(\chi) = \sum_{n=0}^{p-2} \overline{g^n} \rho^{-m(n+b)}, \tag{13}$$

where $\bar{s} \equiv s\, (\mathrm{mod}\, p)$ and $0 \leqslant \bar{s} < p$ with $\chi = \chi_0^m$ and m odd. Applying μ_a to (13), we find that

$$(\chi(2l)\, S(\chi))^{\mu_a} = \sum_{n=0}^{p-2} \overline{g^n} \rho^{-ma(n+b)}. \tag{14}$$

As a is odd, it follows that $ma \equiv w \pmod{p-1}$ with w odd. That is,

$$(\chi_0{}^m(2l)\, S(\chi_0{}^m))^{\mu_a} = \chi_0{}^w(2l)\, S(\chi_0{}^w). \tag{15}$$

As $(a, p-1) = 1$, it follows that μ_a induces a bijection of the set

$$\{\chi_0{}^m(2l)\, S(\chi_0{}^m); \qquad m = 1, 3,..., p-2\}.$$

Hence, x_l is invariant under the automorphisms of $Q(\rho)$ and therefore lies in Q.

Assuming Chowla's Theorem, the x_l are uniquely determined. We show then that the x_l as defined by (12) do, in fact, satisfy (7). The expression

$$\sum_{\chi(-1)=-1} \frac{\bar{\chi}(2l)}{S(\chi)},$$

is meaningful for any $l = 1, 2,..., p-1$. Hence, x_l is meaningful for $l = 1, 2,..., p-1$ with the relation, however, that $x_{p-l} = -x_l$. Consider then

$$\sum_{l=1}^{p-1} x_l \xi_l = \sum_{l=1}^{t} x_l \xi_l + \sum_{l=t+1}^{p-1} x_l \xi_l. \tag{16}$$

As $\xi_{p-l} = -\xi_l$ and $x_{p-l} = -x_l$, it follows from (16) that

$$\sum_{l=1}^{p-1} x_l \xi_l = 2 \sum_{l=1}^{t} x_l \xi_l. \tag{17}$$

Moreover, it is easy to see that

$$\xi_l = 1 + \frac{2}{p} \sum_{k=1}^{p-1} k \xi^{2lk}. \tag{18}$$

This being so, we have (bearing in mind that the sums involving characters are over odd characters) from (17) and (18)

$$\begin{aligned} A &= \sum_{l=1}^{t} x_l \xi_l = \frac{1}{2} \sum_{l=1}^{p-1} x_l \xi_l \\ &= \frac{p\bar{\chi}(2)}{p-1} \left(\sum_{l=1}^{p-1} \sum_{\chi} \frac{\bar{\chi}(l)}{S(\chi)} \left(1 + \frac{2}{p} \sum_{k=1}^{p-1} k \zeta^{2kl} \right) \right) \\ &= \frac{p\bar{\chi}(2)}{p-1} \sum_{\chi} \frac{1}{S(\chi)} \sum_{l=1}^{p-1} \bar{\chi}(l) + \frac{2}{p-1} \sum_{l=1}^{p-1} \sum_{\chi} \frac{\bar{\chi}(l)}{S(\chi)} \sum_{k=1}^{p-1} k \zeta^{2kl}. \end{aligned} \tag{19}$$

As χ is not principal, the first term is 0. In the second sum, we introduce the term $1 = \chi(k)\,\bar{\chi}(k)$ and get from (19)

$$A = \frac{2}{p-1} \sum_{\chi} \frac{1}{S(\chi)} \sum_{k=1}^{p-1} k\chi(k) \sum_{l=1}^{p-1} \bar{\chi}(2kl)\,\zeta^{2kl}.$$

For a given k we have

$$\sum_{l=1}^{n-1} \bar{\chi}(2kl)\,\zeta^{2kl} = \sum_{n=1}^{p-1} \bar{\chi}(n)\,\zeta^{n},$$

and the left sum is therefore independent of k. Hence,

$$A = \frac{2}{p-1} \sum_{\chi} \sum_{n=1}^{p-1} \bar{\chi}(n)\,\zeta^{n} \frac{1}{S(\chi)} \sum_{k=1}^{p-1} k\chi(k)$$

$$= \frac{2}{p-1} \sum_{n=1}^{p-1} \zeta^{n} \sum_{\chi} \bar{\chi}(n). \tag{20}$$

To evaluate the inner sum (which is well known), we note that, if $n \not\equiv 1 \pmod{p}$, then

$$0 = \sum_{k=1}^{p-1} \chi_0{}^{k}(n) = \sum_{m=1}^{t} \chi_0^{2m-1}(n) + \sum_{m=1}^{t} \chi_0^{2m}(n)$$

$$= (1 + \chi_0(n)) \sum_{m=1}^{t} \chi_0^{2m-1}(n).$$

If $\chi_0(n) \neq -1$—i.e., if $n \not\equiv -1 \pmod{p}$—then

$$\sum_{m=1}^{t} \chi_0^{2m-1}(n) = 0.$$

It follows that

$$\sum_{\chi} \bar{\chi}(n) = \begin{cases} 0, & \text{if } n \not\equiv \pm 1 \pmod{p} \\ -t, & \text{if } n \equiv -1 \pmod{p} \\ t, & \text{if } n \equiv 1 \pmod{p}. \end{cases} \tag{21}$$

Applying (21) to (20), we get

$$A = \frac{2}{p-1} (t\zeta - t\zeta^{-1}) = \zeta - \zeta^{-1},$$

as required.

As a corollary, we derive Iwasawa's Theorem. From (12) we have

$$\nu_p(x_l) \geqslant \min_{\chi} \nu_p\left(\frac{p}{S(\chi)}\right) \geqslant -\max_{\chi}\left(\nu_p\left(\frac{S(\chi)}{p}\right)\right), \tag{22}$$

the min and max taken over odd characters. Therefore, from (22)

$$-\nu_p(x_l) \leqslant \max_{\chi} \nu_p\left(\frac{S(\chi)}{p}\right). \tag{23}$$

As the right-hand side does not depend on l, we get from (23),

$$\delta_p \leqslant \max_{\chi} \nu_p\left(\frac{S(\chi)}{p}\right).$$

To prove the reverse inequality, we write (12) in the form

$$[x_1, x_2, \ldots, x_t] = \left(\frac{p}{S(\chi_1)}, \ldots, \frac{p}{S(\chi_t)}\right) M, \tag{23}$$

where M is the matrix $[\bar{\chi}(2l)]$, χ is odd, and $l = 1, 2, \ldots, t$.

The matrix M is nonsingular; in fact, its determinant is prime to p. Since $\bar{\chi} = \chi^{-1}$, we can write M as

$$M = [\chi_0^{-(2k-1)}(2l)].$$

Hence,

$$\begin{aligned} M\overline{M}^T &= [\chi_0^{-(2k-1)}(2l)][\chi_0^{2r-1}(2l)] \\ &= \left[\sum_{l=1}^{t} \chi_0^{2r-2k}(2l)\right]. \end{aligned}$$

If $r = k$, this term of the matrix has value t. If $r \neq k$, then $\chi_0^{2(r-k)}$ is an even character, not the principal one, and it is easily seen that then the value is 0. Therefore, $M\overline{M}^T = tI$. That is, M is nonsingular and

$$\det(M\overline{M}^T) = t^t$$

or

$$|\det M|^2 = t^t.$$

In other words, $\nu_p(\det M) = 0$, as is easily seen.

Therefore, from (23)

$$\frac{p}{S(\chi)} = \frac{1}{\det M}\sum_{l=1}^{t} \alpha_l x_l, \tag{24}$$

where $\alpha_l \in Z[\rho]$.

Consequently, from (24)

$$\nu_p\left(\frac{p}{S(\chi)}\right) \geqslant \min \nu_p(x_l),$$

$$\nu_p\left(\frac{S(\chi)}{p}\right) \leqslant \max(-\nu_p(x_l)) = \delta_p .$$

Hence, $\max \nu_p(S(\chi)/p) \leqslant \delta_p$. This completes the proof.

3. Derivation of (12) and Alternate Proof of Chowla's Theorem

We begin with the easily proved identity

$$\sum_{n=1}^{p-1} n\zeta^n = \frac{p}{\zeta - 1}. \tag{25}$$

Replacing ζ by ζ^{-1}, we get

$$\sum_{n=1}^{p-1} n\zeta^{-n} = \frac{-p\zeta}{\zeta - 1}. \tag{26}$$

Subtracting (26) from (25) and replacing ζ by ζ^2, we deduce that

$$\sum_{n=1}^{p-1} n(\zeta^{2n} - \zeta^{-2n}) = p\left(\frac{\zeta + \zeta^{-1}}{\zeta - \zeta^{-1}}\right) = p\xi_1 . \tag{27}$$

Applying the automorphisms $\zeta \to \zeta^a$ $(a = 1, 2,..., t)$, we infer that

$$\sum_{n=1}^{p-1} n(\zeta^{2an} - \zeta^{-2an}) = p\xi_a \qquad (a = 1, 2,..., t). \tag{28}$$

The automorphisms $\zeta \to \zeta^a$ $(a = t + 1,..., p - 1)$ yield nothing new.

We shall cut the summation in (28) to t. Let $\bar{x}$ denote the residue of x modulo p with $0 \leqslant \bar{x} < p$. Determine a such that $an \equiv m \pmod p$; i.e., $n \equiv ma^{-1} \pmod p$. Then from (28), we get

$$\begin{aligned} p\xi_a &= \sum_{m=1}^{p-1} \overline{ma^{-1}}(\zeta^{2m} - \zeta^{-2m}) \\ &= \left(\sum_{m=1}^{t} + \sum_{m=t+1}^{p-1}\right) (\overline{ma^{-1}}(\zeta^{2m} - \zeta^{-2m})) \\ &= S_1 + S_2 . \end{aligned} \tag{29}$$

In S_2, put $k = p - m$; then

$$S_2 = \sum_{k=1}^{t} (\overline{(p-k)(a^{-1})})(\zeta^{-2k} - \zeta^{2k})$$

$$= \sum_{k=1}^{t} (p - \overline{ka^{-1}})(\zeta^{-2k} - \zeta^{2k}). \tag{30}$$

Combining (29) and (30), we get

$$p\xi_a = -\sum_{m=1}^{t} (2\overline{ma^{-1}} - p)(\zeta^{p-2m} - \zeta^{-(p-2m)}) \qquad (a = 1, 2, ..., t). \tag{31}$$

Let $\boldsymbol{\xi} = [\xi_1, \xi_2, ..., \xi_t]$ and

$$\begin{aligned}\boldsymbol{\alpha} &= [\zeta^{p-2} - \zeta^{-(p-2)}, \zeta^{p-4} - \zeta^{-(p-4)}, ..., \zeta - \zeta^{-1}] \\ &= [\alpha_t, \alpha_{t-1}, ..., \alpha_1],\end{aligned}$$

where $\alpha_i = \zeta^{2i-1} - \zeta^{-(2i-1)}$, $i = 1, 2, ..., t$.

From (31), we get the matrix equation

$$-p\boldsymbol{\xi} = \boldsymbol{\alpha}A, \tag{32}$$

where

$$A = [2(\overline{ma^{-1}}) - p] \qquad (m = 1, 2, ..., t,\ a = 1, 2, ..., t). \tag{33}$$

Now, if the α_i are linearly independent, then the ξ_i are linearly independent if and only if A is nonsingular. We shall show that the α_i are linearly independent and we shall show that A is nonsingular—indeed, we shall find its inverse.

To see the first statement, assume that there exist $c_l \in Q$ $(l = 1, 2, ..., t)$ such that

$$\sum_{l=1}^{t} c_l \alpha_l = 0.$$

Define $c_{p-l} = -c_l$. Then we can rewrite this equation as

$$\sum_{l=1}^{t} c_l \zeta^{2l-1} + \sum_{l=1}^{t} c_{p-l} \zeta^{p-(2l-1)} = 0$$

or

$$\sum_{j=1}^{p-1} d_j \zeta^j = 0.$$

This contradicts the fact that ζ has degree $p-1$ unless $d_j = 0, j = 1,..., p-1$.

The matrix A has rational coefficients; to find x_l, it therefore suffices to find A^{-1}—in fact; it is enough to find the last column of A^{-1}.

Chowla's Theorem will then follow.

We now invert A. The argument is based on an idea from a paper of Carlitz and Olson [3].

For any integer c let

$$\{c\} = 2\bar{c} - p; \tag{34}$$

then it follows at once that $\{c\}$ is odd, $|\{c\}| \leqslant p-2$, and that

$$\{-c\} = -\{c\}. \tag{35}$$

Thus, as c runs from 1 to t, $\{c\}$ runs through $1, 3,..., p-2$ with possible sign changes.

Let g be a primitive root mod p; then $\{g^k\}$ $(k = 0, 2,..., t-1)$ are all distinct and coincide with $\{a\}$ $(a = 1,..., t)$ except for order and sign. In fact, if $1 \leqslant c \leqslant t$, then

$$c \equiv \epsilon_c \overline{g^{i_c}} \pmod{p} \tag{36}$$

with $0 \leqslant i_c < t$ and

$$\epsilon_c = \begin{cases} 1, & \text{if } \overline{g^{i_c}} < \frac{p}{2} \\ -1, & \text{if } \overline{g^{i_c}} > \frac{p}{2}. \end{cases}$$

This follows from the fact that $g^t \equiv -1 \pmod{p}$. Moreover, if

$$\{c\} = \epsilon_c\{g^{i_c}\},$$

then $\{c^{-1}\} = \epsilon_c\{g^{-i_c}\}$. There exists therefore a permutation matrix M and a sign change K such that

$$[\{1^{-1}\}, \{2^{-1}\},..., \{t^{-1}\}] = [\{g^{-0}\}, \{g^{-1}\},..., \{g^{-(t-1)}\}]\, MK; \tag{37}$$

then

$$[\{m1^{-1}\}, \{m2^{-1}\},..., \{mt^{-1}\}] = [\{mg^{-0}\}, \{mg^{-1}\},..., \{mg^{-(t-1)}\}]\, MK. \tag{38}$$

Putting $MK = P$, we get from (38)

$$[\{ma^{-1}\}] = P^T[\{g^{i-j}\}]\, P. \tag{39}$$

Let $B = [\{g^{i-j}\}]$; then (39) becomes

$$A = P^T B P. \tag{40}$$

We shall invert A by diagonalizing B. Let ρ be a primitive $(p-1)$-st root of unity and let

$$C = [\delta_{ij}\rho^j] \quad (i, j = 0,\ldots, t-1).$$

Then

$$CB\bar{C} = [\{g^{i-j}\}\,\rho^{i-j}]. \tag{41}$$

The first row of this matrix is

$$[\{g^{-0}\}\,\rho^{-0}, \{g^{-1}\}\,\rho^{-1},\ldots, \{g^{-(t-1)}\}\,\rho^{-(t-1)}].$$

Because $g^t \equiv -1 \pmod p$, $\rho^t = -1$, we get from (35) that the second row is

$$[\{g^{-(t-1)}\}\,\rho^{-(t-1)}, \{g^{-0}\}\,\rho^{-0},\ldots, \{g^{-(t-2)}\}\,\rho^{-(t-2)}],$$

and so on inductively. Thus, $CB\bar{C}$ is a circular matrix; i.e., the rows are permutations of the first row obtained by powers of the cyclic permutation $(1, 2,\ldots, t)$. To diagonalize $CB\bar{C}$, let λ be a primitive tth root of unity. Then $\lambda = \rho^2$, and let

$$L = [\lambda^{ij}] \qquad (i, j = 0,\ldots, t-1).$$

Suppose that the first row of $CB\bar{C}$ is denoted by $[a_0, a_1,\ldots, a_{t-1}]$ so that the element of the ith row and jth column (counting from 0) is given by a_{t+j-i}, it being understood that the subscripts are reduced to the least nonnegative residue modulo t. Hence,

$$\begin{aligned}\bar{L}CB\bar{C}L &= [\lambda^{-ij}][a_{t-i+j}][\lambda^{ij}] \\ &= [\lambda^{-ij}]\left[\sum_{k=0}^{t-1} a_{t-i+k}\lambda^{kj}\right].\end{aligned}$$

But

$$\begin{aligned}\sum_{k=0}^{t-1} a_{t-i+k}\lambda^{kj} &= \sum_{m=0}^{t-1} a_m\lambda^{(m+i)j} \\ &= \lambda^{ij}\sum_{m=0}^{t-1} a_m\lambda^{mj}.\end{aligned}$$

Therefore,

$$\bar{L}CB\bar{C}L = \left[\sum_{k=0}^{t-1} \lambda^{-ik}\lambda^{kj} \sum_{m=0}^{t-1} a_m\lambda^{mj}\right]$$

$$= \left[t\delta_{ij} \sum_{m=0}^{t-1} a_m\lambda^{mj}\right]. \tag{42}$$

On the other hand,

$$\sum_{m=0}^{t-1} a_m\lambda^{mj} = \sum_{m=0}^{t-1} \{g^{-m}\}\, \rho^{-m}\rho^{2mj}$$

$$= \sum_{m=0}^{t-1} \{g^{-m}\}\, \rho^{m(2j-1)}.$$

Moreover,

$$\sum_{m=0}^{p-2} \{g^{-m}\}\, \rho^{m(2j-1)} = \left(\sum_{m=0}^{t-1} + \sum_{m=t}^{p-2}\right)(\{g^{-m}\}\, \rho^{m(2j-1)}). \tag{43}$$

Replacing m by $n + t$ in the second sum and noting that

$$g^t \equiv -1 \pmod p, \qquad \rho^t = -1, \qquad \text{and} \quad \{-c\} = -\{c\},$$

we get from (43)

$$\sum_{m=0}^{p-2} \{g^{-m}\}\, \rho^{m(2j-1)} = 2 \sum_{m=0}^{t-1} \{g^{-m}\}\, \rho^{m(2j-1)}. \tag{44}$$

Furthermore,

$$\sum_{m=0}^{p-2} \{g^{-m}\}\, \rho^{m(2j-1)} = 2 \sum_{m=0}^{p-2} \overline{g^{-m}}\rho^{m(2j-1)}. \tag{45}$$

Thus from (44) and (45), we get

$$\sum_{m=0}^{t-1} \{g^{-m}\}\, \rho^{m(2j-1)} = \sum_{m=0}^{p-2} \overline{g^{-m}}\rho^{m(2j-1)}$$

$$= S(\chi_0^{2j-1}). \tag{46}$$

Collecting our results, we find from (40)–(42), and (46),

$$[CP^TAP\bar{C}L = t[\delta_{ij}S(\chi_0^{2j-1})] \qquad (i, j = 0,\ldots, t-1). \tag{47}$$

Therefore,

$$t^{-1}P^{T}AP = C^{-1}\bar{L}^{-1}[\delta_{ij}S(\chi_0^{2j-1})]\, L^{-1}\bar{C}^{-1}.$$

We remarked above that $S(\chi_0^{2j-1}) \neq 0$; hence,

$$\begin{aligned} tP^{-1}A^{-1}(P^{T})^{-1} &= \bar{C}L[\delta_{ij}S^{-1}(\chi_0^{2j-1})]\, \bar{L}C \\ &= [\delta_{ij}\rho^{-j}][\rho^{2ij}][\delta_{ij}S^{-1}\chi_0^{2j-1})][\rho^{-2ij}][\delta_{ij}\rho^{i}] \\ &= [\rho^{i(2j-1)}][\delta_{ij}S^{-1}(\chi_0^{2j-1})][\rho^{-(2i-1)j}] \\ &= [\rho^{i(2j-1)}S^{-1}(\chi_0^{2j-1})][\rho^{-(2i-1)j}] \\ &= \left[\sum_{k=0}^{t-1} \rho^{i(2k-1)}S^{-1}(\chi_0^{2k-1})\, \rho^{-(2k-1)j}\right] \\ &= \left[\sum_{k=0}^{t-1} S^{-1}(\chi_0^{2k-1})\, \chi_0^{-(2k-1)}(\{g^{i-j}\})\, \chi_0^{2k-1}(2)\right]. \end{aligned}$$

Since $P^{-1} = P^{T}$, we get

$$\begin{aligned} A^{-1} &= t^{-1}\left[\sum_{k=0}^{t-1} S^{-1}(\chi_0^{2k-1})\, \chi_0^{-(2k-1)}(\{ma^{-1}\})\, \chi_0^{2k-1}(2)\right] \\ &= t^{-1}\left[\sum_{k=0}^{t-1} S^{-1}(\chi_0^{2k-1})\, \chi_0^{-(2k-1)}(ma^{-1})\right]. \end{aligned}$$

From (32), we have $\boldsymbol{\alpha} = -p\xi A^{-1}$. Therefore,

$$\zeta - \zeta^{-1} = \frac{-2p}{p-1}\sum_{m=1}^{t} \xi_m \left(\sum_{k=0}^{t-1} S^{-1}(\chi_0^{2k-1})\, \chi_0^{-(2k-1)}(mt^{-1})\right).$$

But $t^{-1} = ((p-1)/2)^{-1} \equiv -2 \pmod p$ and, since $\chi(-1) = -1$, we have (replacing χ_0 by a generic χ)

$$\zeta - \zeta^{-1} = \frac{2p}{p-1}\sum_{m=1}^{t} \xi_m \left(\sum_{\chi} S^{-1}(\chi)\, \bar{\chi}(2m)\right). \tag{48}$$

The summation is over all χ for which $\chi(-1) = -1$. Furthermore, in general,

$$\zeta^{a} - \zeta^{-a} = \frac{2p\chi(a)}{p-1}\sum_{m=1}^{t} \xi_m \left(\sum_{\chi} S^{-1}(\chi)\, \bar{\chi}(m)\right) \tag{49}$$

for $a = 1, 2, \ldots, t$.

That is, since $\zeta^a - \zeta^{-a} \in K^-$, there exist $c_l \in Q$ such that

$$\zeta^a - \zeta^{-a} = \sum_{l=1}^{t} c_l \xi_l ,$$

and these c_l are given by

$$c_l = \frac{2p\chi(a)}{p-1} \sum_{\chi} S^{-1}(\chi)\, \bar{\chi}(l),$$

the summation being over odd characters.

Acknowledgments

I should like to acknowledge gratefully the helpful suggestions of my colleagues G. Andrews and S. Chowla. Andrews performed some calculations which confirmed a conjecture on the value of a determinant. He also called my attention to the paper of Carlitz and Olson [3].

References

1. K. Iwasawa, On a theorem of S. Chowla, *J. Number Theory* **7** (1975), 105–107.
2. S. Chowla, The nonexistence of nontrivial linear relations between the roots of a certain irreducible equation, *J. Number Theory* **2** (1970), 120–123.
3. L. Carlitz and F. R. Olson, Maillet's Determinant, *Proc. Amer. Math. Soc.* **6**, 265–269.

Printed in Belgium