NIEUW ARCHIEF VOOR WISKUNDE (3), XXIII (1975), 131-144

LINEAR INDEPENDENCE OF COSECANT VALUES

H. JAGER & H.W. LENSTRA jr.

1. INTRODUCTION

Let p be an odd prime and let $m = \frac{1}{2}(p-1)$. It was proved by S. CHOWLA [3], for $p \equiv 3 \pmod 4$ and later by HASSE [6], and by AYOUB [1], [2], for all odd p, that the m numbers

$$\cot \frac{2\pi\ell}{p} , \quad \ell = 1,\ldots,m,$$

are linearly independent over $\mathbb{Q}$. HASSE [6], also proved the analogous result for the m numbers

$$\tan \frac{2\pi\ell}{p} , \quad \ell = 1,\ldots,m.$$

In the first part of this paper we study the similar problem for the cosecant. It turns out that the m numbers

$$\csc \frac{2\pi\ell}{p} , \quad \ell = 1,\ldots,m, \tag{1}$$

are not always linearly independent over $\mathbb{Q}$. We shall characterize, partly by congruence properties, partly by algebraic properties, those primes p for which the numbers (1) are linearly independent over $\mathbb{Q}$, see theorem 1. Then we give a set of m numbers in terms of the cosecant, viz.

$$\csc^2 \frac{2\pi\ell}{p} , \quad \ell = 1,\ldots,m,$$

which form, for every odd prime p, a $\mathbb{Q}$-linearly independent set of numbers, see theorem 2. Our first proofs of these results are analytical, using among others the partial fraction expansions of the csc and the $\csc^2$, the functional equation for L-functions and the expressions for $L(0;\chi)$ and $L(-1;\chi)$ in terms of the generalized Bernoulli numbers. In the second part we consider the problem from an algebraic point of view, cf. also [6]. This algebraic approach reveals, in our opinion, much more the real nature of the problem. It leads to the general theorem 3, of which the theorems 1 and 2 are special instances. Moreover it contains Chowla's theorem for the cot and Hasse's for the tan.

2. TWO THEOREMS ON THE COSECANT

The analogue for the csc of Chowla's theorem on the cot reads as follows:

THEOREM 1. *Let* p *denote an odd prime and let* $m = \frac{1}{2}(p-1)$. *The* m *numbers*

$$\csc \frac{2\pi\ell}{p}, \quad \ell = 1,\ldots,m,$$

are linearly independent over $\mathbb{Q}$, *if and only if the multiplicative order of* 2 (mod p) *is even.*

PROOF. The starting point of the proof is the partial fraction expansion of the csc, viz.

$$\csc z = \frac{1}{z} + 2z \sum_{n=1}^{\infty} \frac{(-1)^n}{z^2 - n^2\pi^2}, \quad z \neq 0, \pm\pi, \ldots .$$

Putting $z = \frac{2\pi\ell}{p}$, $\ell = 1,\ldots,m$, one obtains

$$\frac{\pi}{p} \csc \frac{2\pi\ell}{p} = \frac{1}{2\ell} + \sum_{n=1}^{\infty} \left(\frac{(-1)^n}{np+2\ell} - \frac{(-1)^n}{np-2\ell}\right).$$

By means of the well known orthogonality property of characters,

$$\frac{1}{p-1}\sum_{\chi\in\hat{G}}\bar{\chi}(k)\chi(a) = 1,\ 0,$$

according to $k \equiv a \pmod p$ and $k \not\equiv a \pmod p$ respectively, where $\hat{G}$ denotes the group of all Dirichlet characters to the modulus p, we see that

$$\frac{\pi}{p}\csc\frac{2\pi\ell}{p} = \frac{1}{p-1}\sum_{\chi\in\hat{G}}\sum_{k=1}^{\infty}\left(\frac{(-1)^{k-}\chi(k)\chi(2\ell)}{k} - \frac{(-1)^{k-}\chi(k)\chi(-2\ell)}{k}\right) =$$

$$= \frac{2}{p-1}\sum_{\chi\in\hat{G}'}\chi(2\ell)\sum_{k=1}^{\infty}\frac{(-1)^{k-}\chi(k)}{k},\quad \ell = 1,\ldots,m,$$

where $\hat{G}'$ denotes the subset of $\hat{G}$ of the so-called *odd* characters, that are the characters for which $\chi(-1) = -1$. Note that we used that $k = np \pm 2\ell$ and n always have the same parity.

Now

$$\sum_{k=1}^{\infty}\frac{(-1)^{k}\chi(k)}{k} = (\chi(2)-1)L(1;\chi)$$

and therefore

$$\csc\frac{2\pi\ell}{p} = \frac{2p}{\pi(p-1)}\sum_{\chi\in\hat{G}'}\chi(2\ell)(\bar{\chi}(2)-1)L(1;\bar{\chi}),\quad \ell = 1,\ldots,m.$$

From the functional equation for $L(s;\chi)$ with $\chi \in \hat{G}'$, see e.g. [7], p.5, it follows that

$$L(1;\bar{\chi}) = -\frac{\pi i}{p}\tau(\bar{\chi})\,L(0;\chi), \tag{2}$$

where $\tau(\chi)$ denotes the ordinary Gauss sum $\sum_{t=1}^{p-1}\chi(t)e^{\frac{2\pi it}{p}}$. Hence

$$\csc\frac{2\pi\ell}{p} = -\frac{2i}{p-1}\sum_{\chi\in\hat{G}'}\chi(2\ell)(\bar{\chi}(2)-1)\tau(\bar{\chi})L(0;\chi),\quad \ell = 1,\ldots,m.$$

The generalized Bernoulli numbers $B_{n,\chi}$, $n = 0,1,\ldots$, χ a primitive Dirichlet character to the modulus f, are defined by

$$\sum_{t=1}^{f-1}\frac{\chi(t)ze^{tz}}{e^{fz}-1} = \sum_{n=0}^{\infty}B_{n,\chi}\frac{z^{n}}{n!}$$

and one has

$$L(1-n;\chi) = -\frac{1}{n} B_{n,\chi}, \tag{3}$$

see [7], §2, theorem 1. This yields our final expression for $\csc \frac{2\pi\ell}{p}$, viz.

$$\csc \frac{2\pi\ell}{p} = \frac{2i}{p-1} \sum_{\chi\in\hat{G}'} \chi(2\ell)(\bar{\chi}(2)-1)B_{1,\chi}\,\tau(\bar{\chi}),\ \ell = 1,\ldots,m. \tag{4}$$

Now the proof is finished in the same way as AYOUB's proof in [1] of Chowla's theorem. Suppose that the m rational numbers $c_\ell, \ell = 1,\ldots,m$, are such that

$$\sum_{\ell=1}^{m} c_\ell \csc \frac{2\pi\ell}{p} = 0.$$

In view of (4) this implies

$$\sum_{\chi\in\hat{G}'} [(\bar{\chi}(2)-1)B_{1,\chi} \sum_{\ell=1}^{m} c_\ell\chi(\ell)]\,\tau(\bar{\chi}) = 0. \tag{5}$$

From the definition of the numbers $B_{n,\chi}$ it follows that with χ a non-principal character to the modulus p,

$$B_{n,\chi} \in \mathbb{Q}(e^{\frac{2\pi i}{p-1}}).$$

In fact, for the numbers $B_{1,\chi}$ we have

$$B_{1,\chi} = \frac{1}{p} \sum_{t=1}^{p-1} \chi(t)t,\ \chi \text{ non-principal}, \tag{6}$$

which follows from IWASAWA [7], p.10, last formula. Hence the whole expression between square brackets in (5) belongs to the field $\mathbb{Q}(e^{\frac{2\pi i}{p-1}})$. But, as AYOUB showed in [1], the numbers

$$\tau(\chi),\ \chi \in \hat{G},$$

are linearly independent over this field. Thus

$$(\bar{\chi}(2)-1)B_{1,\chi} \sum_{\ell=1}^{m} c_\ell \chi(\ell) = 0, \ \chi \in \hat{G}'.$$

From (2), (3) and from $L(1;\chi) \neq 0$ we see that

$$B_{1,\chi} \neq 0, \ \chi \in \hat{G}' \tag{7}$$

and hence that

$$(\bar{\chi}(2)-1) \sum_{\ell=1}^{m} c_\ell \chi(\ell) = 0, \ \chi \in \hat{G}'.$$

Let p be a prime for which the multiplicative order k of 2 (mod p) is even, say $k = 2\kappa$. Then $2^K \equiv -1 \pmod{p}$ and therefore $(\chi(2))^K = \chi(-1) = -1$, $\chi \in \hat{G}'$. Hence for those p we always have $\chi(2) \neq 1$, $\chi \in \hat{G}'$ and thus

$$\sum_{\ell=1}^{m} c_\ell \chi(\ell) = 0, \ \chi \in \hat{G}'.$$

Since the matrix

$$(\chi(\ell)), \ \ell = 1,\ldots,m, \ \chi \in \hat{G}',$$

is non-singular we must have

$$c_\ell = 0, \ \ell = 1,\ldots,m,$$

which proves the if-part of theorem 1.

Suppose now that the order k of 2 (mod p) is odd; hence $k \leq m$. For every complex number ζ with $\zeta \neq 0, \pm 1, \pm i$, one has

$$\zeta(\zeta-\zeta^{-1})^{-1} = (\zeta^2-\zeta^{-2})^{-1} + \zeta^2(\zeta^2-\zeta^{-2})^{-1}. \tag{8}$$

A repeated application of (8) on its own last term yields, with ζ a primitive p-th root of unity,

$$\zeta(\zeta-\zeta^{-1})^{-1} = \sum_{j=1}^{k} (\zeta^{2^j}-\zeta^{-2^j})^{-1} + \zeta^{2^k}(\zeta^{2^k}-\zeta^{-2^k})^{-1}$$

or

$$\sum_{j=0}^{k-1} (\zeta^{2^j}-\zeta^{-2^j})^{-1} = 0. \tag{9}$$

Observing that -1 is not contained in the multiplicative group generated by 2, modulo p, and that the cosecant is an odd function, we see that (9) is nothing else than a relation

$$\sum_{\ell=1}^{m} c_\ell \csc \frac{2\pi\ell}{p} = 0, \quad c_\ell = 0, \pm 1, \text{ not all } c_\ell = 0, \quad \ell = 1,\ldots,m.$$

□

In their studies on the representation of -1 as a sum of squares, FEIN, GORDON & SMITH [5] and CONNELL [4], characterized the primes p for which the condition of our theorem 1 is fulfilled. It is easy to see that for $p \equiv 3, 5 \pmod 8$, the order of 2 (mod p) is always even and that for $p \equiv 7 \pmod 8$ this order is always odd. In [4] and [5] one finds a calculation of the asymptotic density of the primes p for which the order of 2 is even, among all odd primes. This density is 17/24.

For every odd prime p a set of m $\mathbb{Q}$-linearly independent numbers, in terms of values of the cosecant, is given by the following

THEOREM 2. *Let* p *denote an odd prime and let* $m = \frac{1}{2}(p-1)$. *Then the* m *numbers*

$$\csc^2 \frac{2\pi\ell}{p}, \quad \ell = 1,\ldots,m,$$

are linearly independent over $\mathbb{Q}$.

PROOF. The proof is quite similar to that of theorem 1. Starting with

$$\csc^2 z = \sum_{n=-\infty}^{\infty} \frac{1}{(z-n\pi)^2}, \quad z \neq 0, \pm\pi, \ldots,$$

one easily gets

$$\csc^2 \frac{2\pi\ell}{p} = \frac{2p^2}{\pi^2(p-1)} \sum_{\chi\in\hat{G}"} \chi(2\ell)L(2;\bar{\chi}), \quad \ell = 1,\ldots,m,$$

where $\hat{G}"$ denotes the subgroup of index 2 of $\hat{G}$ of all *even* characters to the modulus p, where even means that $\chi(-1) = 1$. The unit character of $\hat{G}$ will in the sequel be denoted by χ_0.

From the functional equation for $L(s;\chi)$ with $\chi \in \hat{G}"$, $\chi \neq \chi_0$, see e.g. [7], p.5, it follows that

$$L(2;\bar{\chi}) = -\frac{2\pi^2}{p^2}\tau(\bar{\chi})L(-1;\chi)$$

and hence, with (3), that

$$L(2;\bar{\chi}) = \frac{\pi^2}{p^2}\tau(\bar{\chi})B_{2,\chi}, \quad \chi \in \hat{G}", \ \chi \neq \chi_0. \tag{10}$$

Further,

$$L(2;\chi_0) = (1 - \frac{1}{p^2})\zeta(2) = (1 - \frac{1}{p^2})\frac{\pi^2}{6}$$

and so, in view of $\tau(\chi_0) = -1$,

$$L(2;\chi_0) = \frac{\pi^2}{p^2}\frac{1 - p^2}{6}\tau(\chi_0). \tag{11}$$

Now if we define for abbreviation the numbers C_χ, $\chi \in \hat{G}"$, by

$$C_\chi = \begin{cases} B_{2,\chi}, & \chi \neq \chi_0 \\ \frac{1-p^2}{6}, & \chi = \chi_0 \end{cases},$$

we can combine (10) and (11) to

$$L(2;\bar{\chi}) = \frac{\pi^2}{p^2} C_\chi \tau(\bar{\chi}), \quad \chi \in \hat{G}".$$

Clearly,

$$C_\chi \in \mathbb{Q}(e^{\frac{2\pi i}{p-1}}),\ C_\chi \neq 0,\ \chi \in \hat{G}''.$$

For future use we note the following analogue to (6), which follows from [7], p.10:

$$C_\chi = \frac{1}{p}\sum_{t=1}^{p-1} \chi(t)t^2,\ \chi \neq \chi_0. \tag{12}$$

So we have found the following expression for $\csc^2 \frac{2\pi\ell}{p}$:

$$\csc^2 \frac{2\pi\ell}{p} = \frac{2}{p-1} \sum_{\chi\in\hat{G}''} \chi(2\ell)\ C_\chi \tau(\bar{\chi}),\ \ell = 1,\ldots,m.$$

From this, every relation

$$\sum_{\ell=1}^{m} c_\ell \csc^2 \frac{2\pi\ell}{p} = 0,\ c_\ell \in \mathbb{Q},\ \ell = 1,\ldots,m,$$

leads to

$$\sum_{\ell=1}^{m} c_\ell \chi(\ell) = 0,\ \chi \in \hat{G}''$$

and since the matrix

$$(\chi(\ell)),\ \ell = 1,\ldots,m,\ \chi \in \hat{G}''$$

is non-singular, this is only possible when $c_\ell = 0$, $\ell = 1,\ldots,m$. □

3. AN ALGEBRAIC APPROACH

We consider a more general problem. Let K be a field, G a finite abelian group of order n, with n prime to the characteristic of K, and M a module over the group ring K[G]. For $\alpha \in M$ we are interested in calculating the K-dimension of $K[G].\alpha = \{r.\alpha \mid r \in K[G]\}$ and, more generally, in finding all K-linear relations between the elements $\sigma\alpha$,

$\sigma \in G$.

Define the map $K[G] \to M$ by sending r to $r\alpha$, for $r \in K[G]$. The kernel I of this map is called the *annihilator* of α. It is an ideal of $K[G]$ which can be viewed as the space of linear relations between the elements $\sigma\alpha$, $\sigma \in G$. Obviously, $\dim_K K[G].\alpha = n - \dim_K I$; so the question is how to determine I.

First we consider the case that K contains all e-th roots of unity, where e is the exponent of G. Then the group of characters

$$\hat{G} = \{\chi: G \to K^* \mid \chi \text{ is a group homomorphism}\}$$

has order n. If we put

$$e_\chi = \frac{1}{n} \sum_{\sigma \in G} \chi^{-1}(\sigma)\sigma \in K[G]$$

then the set $\{e_\chi \mid \chi \in \hat{G}\}$ is a K-basis for $K[G]$. More precisely, an element

$$r = \sum_{\sigma \in G} k_\sigma . \sigma$$

of $K[G]$, with $k_\sigma \in K$, has the following representation on the basis $\{e_\chi \mid \chi \in \hat{G}\}$:

$$r = \sum_{\chi \in \hat{G}} \left(\sum_{\sigma \in G} k_\sigma \chi(\sigma) \right) . e_\chi . \tag{13}$$

It is well known and easily proved that multiplication in $K[G]$ is performed componentwise on the basis $\{e_\chi \mid \chi \in \hat{G}\}$:

$$\left(\sum k_\chi e_\chi\right).\left(\sum k'_\chi e_\chi\right) = \sum k_\chi k'_\chi e_\chi$$

for $k_\chi, k'_\chi \in K$. Thus we see that the ring $K[G]$ is isomorphic to the product of n copies of K, with componentwise ring operations. It follows that every ideal J of $K[G]$ has the form

(14) $$J = \sum_{\chi \in S} K.e_\chi$$

for a subset S of $\hat{G}$. So there are precisely 2^n ideals of K[G]. We say that J corresponds to S if (14) holds; clearly $\dim_K(J) = \#S$.

The annihilator I of α now corresponds to

$$\{\chi \in \hat{G} \mid e_\chi \in I\} = \{\chi \in \hat{G} \mid \sum_{\sigma \in G} \chi^{-1}(\sigma)\sigma\alpha = 0\}.$$

We conclude that the space of linear relations between the $\sigma\alpha$, $\sigma \in G$, is completely determined by the set of characters χ for which $\sum_{\sigma \in G} \chi^{-1}(\sigma)\sigma\alpha = 0$ $(\in M)$. In particular we have

$$\dim_K K[G].\alpha = \#\{\chi \in \hat{G} \mid \sum_{\sigma \in G} \chi^{-1}(\sigma)\sigma\alpha \neq 0\}.$$

In order to deal with general K, we choose a field extension $K \subset K'$ such that K' contains all e-th roots of unity, and apply the above results to the K'[G]-module $M' = K' \otimes_K M$. Then the annihilators I and I' of $\alpha (= 1 \otimes \alpha)$ in K[G] and K'[G], respectively, determine each other by

$$I' = K' \otimes I \subset K' \otimes K[G] = K'[G],$$
$$I = I' \cap K[G] \text{ (inside } K'[G]).$$

Further

$$\dim_K I = \dim_{K'} I'$$

and I' corresponds to

$$\{\chi \in \hat{G} \mid \sum_{\sigma \in G} \chi^{-1}(\sigma) \otimes \sigma\alpha = 0\}$$

where $\hat{G}$ is the group of characters $G \to K'^*$.

Conclusion: Let K be a field and G a finite abelian group of order prime to the characteristic of K. Let K' be an extension field of K

containing the e-th roots of unity, with e = exp(G), and let $\hat{G}$ be the group of characters $\chi: G \to K'^*$. Then for every K[G]-module M and every $\alpha \in M$ we have

$$\dim_K K[G].\alpha = \#\{\chi \in \hat{G} \mid \sum_{\sigma \in G} \chi^{-1}(\sigma) \otimes \sigma\alpha \neq 0 \text{ in } K' \otimes_K M\}.$$

Further, the space of linear relations between $\{\sigma\alpha \mid \sigma \in G\}$ is completely determined by the set of $\chi \in \hat{G}$ for which $\sum_{\sigma \in G} \chi^{-1}(\sigma) \otimes \sigma\alpha = 0$.

We apply this to the situation $K = \mathbb{Q}$, $M = \mathbb{Q}(\zeta_p)$ with p prime, and $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$; here ζ_p denotes a primitive p-th root of unity and M is a K[G]-module in an obvious way. We take $K' = \mathbb{C}$.

For $t \in \mathbb{Z}$, $p \nmid t$, let σ_t be the element of G mapping ζ_p to ζ_p^t. Then $G = \{\sigma_t \mid 1 \leq t \leq p-1\}$, and writing $\chi(t)$ for $\chi(\sigma_t)$ we see that $\hat{G}$ can be identified with the set of Dirichlet characters with conductor dividing p.

The condition $\sum_{\sigma \in G} \chi^{-1}(\sigma) \otimes \sigma\alpha = 0$ can be expressed conveniently in terms of the coefficients of a representation

$$\alpha = \sum_{t=1}^{p-1} a_t \zeta_p^t \qquad (a_t \in \mathbb{Q}).$$

Notice that such a representation exists, since $\{\zeta_p^t \mid 1 \leq t \leq p-1\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\zeta_p)$. A short computation shows

$$\sum_{\sigma \in G} \chi^{-1}(\sigma) \otimes \sigma\alpha = \Big(\sum_{t=1}^{p-1} \chi(t) a_t\Big).\Big(\sum_{u=1}^{p-1} \chi^{-1}(u) \otimes \zeta_p^u\Big).$$

The second factor on the right (essentially a Gauss sum) is a nonzero element of M', by the linear independence of $\{\zeta_p^u \mid 1 \leq u \leq p-1\}$ over $\mathbb{Q}$; so

$$\sum_{\sigma \in G} \chi^{-1}(\sigma) \otimes \sigma\alpha = 0 \iff \sum_{t=1}^{p-1} \chi(t) a_t = 0.$$

We have proved:

THEOREM 3. *Let* p *be a prime number, and let* α *be an algebraic number of the form*

$$\alpha = \sum_{t=1}^{p-1} a_t \zeta_p^t$$

with $a_t \in \mathbb{Q}$, $1 \le t \le p-1$, *where* ζ_p *denotes a primitive* p-th *root of unity. Then the dimension of the* $\mathbb{Q}$*-vector space generated by the conjugates of* α *is equal to the number of Dirichlet characters* χ *to the modulus* p *for which* $\sum_{t=1}^{p-1} \chi(t)a_t \neq 0$. *Also, the set of these* χ *completely determines the set of all linear relations between the conjugates of* α.

In order to derive theorem 1 from theorem 3 we can take $\alpha = 2p(\zeta_p - \zeta_p^{-1})^{-1}$, since the set of conjugates of α equals

$$\{\pm ip.\csc(2\pi\ell/p) \mid 1 \le \ell \le m\}.$$

An elementary computation shows

$$\alpha = \sum_{t \text{ odd}} (t-p)\,\zeta_p^t + \sum_{t \text{ even}} t\,\zeta_p^t$$

where t ranges over the odd integers in the set $\{1,2,\ldots,p-1\}$ and over the even ones, respectively. So we must determine for which χ the sum

$$\sum_{t \text{ odd}} \chi(t)(t-p) + \sum_{t \text{ even}} \chi(t)t \tag{15}$$

vanishes. We have

$$\begin{aligned} 2(1-\chi(2)) \sum_{t=1}^{p-1} \chi(t)t &= 2\sum_{t=1}^{p-1} \chi(t)t - 2\sum_{t=1}^{p-1} \chi(2t)t \\ &= 2\sum_{t \text{ even}} \chi(t)(t-\tfrac{1}{2}t) + 2\sum_{t \text{ odd}} \chi(t)(t-\tfrac{1}{2}(t+p)) \\ &= \sum_{t \text{ odd}} \chi(t)(t-p) + \sum_{t \text{ even}} \chi(t)t. \end{aligned}$$

Therefore the sum (15) vanishes if and only if

$$\chi(2) = 1 \quad \text{or} \quad \sum_{t=1}^{p-1} \chi(t)t = 0$$

which by (6), (7) and $B_{1,\chi} = 0$ for $\chi \in \hat{G}''$, $\chi \neq \chi_0$, see [7], p.10, is the same as

$$\chi(2) = 1 \quad \text{or} \quad \chi(-1) = 1.$$

We conclude that the dimension of the $\mathbb{Q}$-vector space generated by the conjugates of α is equal to the number of odd characters χ for which $\chi(2) \neq 1$. So the dimension is m if and only if $\chi(2) \neq 1$ for every odd character, which happens if and only if the multiplicative order of 2 mod p is even.

This proves theorem 1. Theorem 2 is derived by analogous computations, using the non-vanishing of the sum

$$\sum_{t=1}^{p-1} \chi(t)t^2, \quad \chi \in \hat{G}'',$$

cf. (12).

Finally, we determine all linear relations between the conjugates of $\alpha = 2p(\zeta_p - \zeta_p^{-1})^{-1}$, for an odd prime p. If $I' \subset \mathbb{C}[G]$ is the annihilator of $\alpha (= 1 \otimes \alpha)$ then by the above proof I' corresponds to

$$\{\chi \mid \chi(2) = 1 \quad \text{or } \chi(-1) = 1\}. \tag{16}$$

Let J be the ideal of $\mathbb{C}[G]$ generated by $1 + \sigma_{-1}$ and $1 + \sigma_2 + \sigma_2^2 + \ldots + \sigma_2^{k-1}$, where k is the multiplicative order of 2 mod p. We claim that I' = J, and to prove this it suffices to show that J also corresponds to (16).

By (13) we have $e_\chi \in J$ if and only if some $r = \sum_{\sigma \in G} k_\sigma \sigma \in J$ satisfies $\sum_{\sigma \in G} k_\sigma \chi(\sigma) \neq 0$; since J is generated by $1 + \sigma_{-1}$ and $1 + \sigma_2 + \ldots + \sigma_2^{k-1}$, this happens if and only if $1 + \chi(-1) \neq 0$ or $1 + \chi(2) + \ldots + \chi(2)^{k-1} \neq 0$, which in turn is equivalent to $\chi(-1) = 1$ or $\chi(2) = 1$. So indeed J corresponds to the set (16).

It follows that the annihilator I of α in $\mathbb{Q}[G]$ is generated by $1 + \sigma_{-1}$ and $1 + \sigma_2 + \ldots + \sigma_2^{k-1}$. That means

(17) $\alpha + \sigma_{-1}(\alpha) = 0$

(18) $\alpha + \sigma_2(\alpha) + \ldots + \sigma_2^{k-1}(\alpha) = 0,$

and all $\mathbb{Q}$-linear relations between the conjugates of α can be derived from these two by conjugation and linearity. (Further (18) follows from (17) if k is even).

Alternatively, one can prove this by verifying (17) and (18) directly, cf. (9); dimension considerations then show that there cannot be "more" relations.

REFERENCES

[1] AYOUB, R., *On a theorem of S. Chowla*, Journal of Number Theory, 7, 105-107 (1975).

[2] AYOUB, R., *On a theorem of Iwasawa*, Journal of Number Theory, 7, 108-120 (1975).

[3] CHOWLA, S., *The nonexistence of nontrivial linear relations between the roots of a certain irreducible equation*, Journal of Number Theory, 2, 120-123 (1970).

[4] CONNELL, I.G., *The Stufe of number fields*, Math. Zeitschrift, 124, 20-22 (1972).

[5] FEIN, B. & B. GORDON & J.H. SMITH, *On the representation of -1 as a sum of two squares in an algebraic number field*, Journal of Number Theory, 3, 310-315 (1971).

[6] HASSE, H., *On a question of S. Chowla*, Acta Arithmetica, XVIII, 275-280 (1971).

[7] IWASAWA, K., *Lectures on p-adic L-functions*, Annals of Mathematics Studies, Number 74, Princeton, 1972.

(Received, May 22, 1975)

Mathematisch Instituut
Universiteit van Amsterdam