View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

JOURNAL OF NUMBER THEORY 2, 120–123 (1970)

The Nonexistence of Nontrivial Linear Relations between the Roots of a Certain Irreducible Equation

S. CHOWLA

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

Communicated May 12, 1969

Let $x_1, ..., x_n$ be the roots of an irreducible equation of degree n over $\mathbf{Q}$. Under what conditions can we have "nontrivial" relations

$$a_1x_1 + \cdots + a_nx_n = 0 \qquad (a_n \in \mathbf{Q})?$$

In some cases it is shown that the nonexistence of nontrivial relations depends on the nonvanishing of Dirichlet's series $L(s, \chi)$ at $s = 1$, when χ is a character with $\chi(-1) = -1$.

Define, as usual,

$$\cos x = (e^{ix} + e^{-ix})/2,$$

$$\sin x = (e^{ix} - e^{-ix})/2i,$$

$$\cot x = (\cos x)/(\sin x).$$

The quantities $\cot(s\pi/p)$ satisfy an equation of degree $(p - 1)$ with coefficients in $\mathbf{Q}$, irreducible over $\mathbf{Q}$. Writing $x_r = \cot(r\pi/p)$ we see from this equation that (and this is otherwise obvious!)

$$\sum_{1}^{p-1} \cot(r\pi/p) = 0,$$

which is a consequence of the relations

$$x_r + x_s = 0 \qquad (r + s = p).$$

In general, one can ask the question: Given an irreducible equation of degree m, with coefficients in $\mathbf{Q}$, with roots $x_1, ..., x_m$, what are the linear relations

$$a_1x_1 + \cdots + a_mx_m = 0$$

with $a_r \in \mathbf{Q}$?

In the above example $[x_r = \cot(r\pi/p]$, $1 \leqslant r < p)$ we shall show that the only linear relations

$$\sum_{1}^{p-1} a_m x_m = 0 \qquad (a_m \in \mathbf{Q})$$

are, when p is a prime $\equiv 3(4)$, those given by

$$a_r + a_s = 0 \qquad (r + s = p).$$

Curiously, this fact is deducible from the well-known result of Dirichlet that

$$L(1, \chi) = \sum_{1}^{\infty} \frac{\chi(n)}{n} \neq 0,$$

where χ is a character $(\bmod\, p)$, with $\chi(-1) = -1$. As we know, the expression for h_2, the "second factor" of the class number of the cyclotomic field $\mathbf{Q}(e^{2\pi i/p})$, involves the *product* of the above series $L(1, \chi)$ with $\chi(-1) = -1$.

My interest in this theorem goes back to February 9, 1949, when I communicated to Professor C. L. Siegel the following:

THEOREM. *Let p and $(p - 1)/2$ be primes. Let each $f(n) = +1, -1$ or 0. Further $f(n) = -f(-n)$, $f(m) = f(n)$ for $m \equiv n(p)$. Then*

$$\sum_{1}^{\infty} \frac{f(n)}{n} \neq 0$$

unless all $f(n)$ are 0.

Professor Siegel's reply dated February 12, 1949, improved this theorem by, for example, relaxing the condition that $(p - 1)/2$ is also a prime. Also the $f(n)$ may be any integers, not all zero (my proof also allowed this extension). I published Siegel's letter to me in *Det Kongelige Norske Videnskabers Selskabs Forhandlinger* **37** (1964), 85–87, after a lapse of 15 years!

Now I can prove Siegel's extension (at least in a special case) in a much more natural manner than he did. In fact let g be a primitive root mod p, where p is a prime $\equiv 3(4)$. Write

$$x_m = \cot(g^{2m}\pi/p) \tag{1}$$

for $1 \leqslant m \leqslant (p - 1)/2$. If possible, assume a relation

$$\sum_{m=1}^{(p-1)/2} f(g^{2m}) x_m = 0 \tag{2}$$

where the f's, as above, are periodic mod p, $f(-n) = -f(n)$, integers, and not all zero. Since the numbers $\pm x_m$ satisfy an irreducible equation over $\mathbf{Q}$ of degree $(p-1)$ we see that

$$x_2 = \varphi(x_1), \quad x_3 = \varphi(x_2), \ldots, x_{(p-1)/2} = \varphi(x_{(p-3)/2})$$

and (3)

$$x_1 = \varphi(x_{(p-1)/2}),$$

where $\varphi(x)$ is a polynomial, over $\mathbf{Q}$, of degree $\leqslant p-2$. We write (2) as

$$a_1 x_1 + a_2 x_2 + \cdots + a_q x_q = 0, \tag{4}$$

where $q = (p-1)/2$.

By Galois theory for the cyclotomic field $\mathbf{Q}(e^{2\pi i/p})$, (4) and (3) give

$$a_1 x_{1+t} + a_2 x_{2+t} + \cdots + a_q x_{q+t} = 0, \tag{5}$$

where $0 \leqslant t < g$ and the subscripts of the x's are taken mod g.

Since the a's are, by supposition, not all zero we see from (5) that the circulant determinant

$$\begin{vmatrix} x_1 & x_2 & \cdots & x_{(p-1)/2} \\ x_2 & x_3 & \cdots & x_1 \\ x_3 & x_4 & \cdots & x_2 \\ \cdots & \cdots & \cdots & \cdots \\ x_{(p-1)/2} & x_1 & \cdots & x_{(p-3)/2} \end{vmatrix}$$

must be 0. As is well known, this circulant determinant factorizes into a product of $q = (p-1)/2$ factors, namely

$$\omega^r x_1 + \omega^{2r} x_2 + \omega^{3r} x_3 + \cdots + \omega^{rq} x_q, \tag{6}$$

where $1 \leqslant r \leqslant q$, and $\omega = e^{2\pi i/q}$.

Now, and here is the surprise, the expressions (6) are precisely the values (except for trivial nonzero factors) of the series

$$L(1, \chi) = \sum_1^\infty \frac{\chi(n)}{n} \tag{7}$$

for all the characters χ with $\chi(-1) = -1$.

Since all the series (7) with $\chi(-1) = -1$ are nonzero, it follows that our circulant determinant is not zero. Hence for $p \equiv 3 (\text{mod } 4)$ there exists no linear relation

$$\sum_{r=1}^{(p-1)/2} a_r \cot(r\pi/p) = 0$$

with the $a_r \in \mathbf{Z}$, unless each $a_r = 0$. This is the theorem we wished to prove. We repeat that p, here, is a prime $\equiv 3(4)$.

Acknowledgments

This paper owes much to the letter of C. L. Siegel quoted above, and also to a letter from A. Weil to the author.

Printed in Belgium