REMARK ON THE PRECEDING PAPER ALGEBRAIC EQUATIONS SATISFIED BY ROOTS OF NATURAL NUMBERS

E. G. STRAUS AND O. TAUSSKY

In the preceding paper [1] it was shown that the polynomials in question are factors of $\Phi_h(x^k/n)$ where Φ_h is the cyclotomic polynomial of order h and k, n are positive integers. The case $k=2$ was settled in [1, Lemma 2]. It will now be shown that this is essentially the only nontrivial case. For a different treatment of a somewhat related question see K. T. Vahlen [2].

First let us remark that we can exclude the case $n=m^d$ where d/k, $d>1$; since we may then set $y=x^{k/d}/m$ so that $\Phi_h(y^d)$ is either reducible with cyclotomic factors or equal to $\Phi_{hd}(y)$. We shall refer to n and $\Phi_h(x^k/n)$ which satisfy the above exclusion as *simplified*.

THEOREM. *The simplified polynomial $\Phi_h(x^k/n)$ is irreducible for all odd k. For $k=2l$ the polynomial is reducible if and only if $\Phi_h(x^2/n)$ is reducible. In that case we have*

$$\Phi_h(x^k/n)=g(x^l)g(-x^l)\,, \tag{1}$$

where the polynomials on the right are irreducible.

The proof is based on the following lemma.

LEMMA. *If $k>2$ and $n^{1/k}$ is simplified then $n^{1/k}$ is not contained in a cyclotomic field.*

Proof. The Galois group of a cyclotomic field $R(\zeta)$ is Abelian and hence all subfields of $R(\zeta)$ are normal. The field $R(n^{1/k})$ is, however, not a normal field for $k>2$.

We can now prove the Theorem. Let ζ_h be a primitive hth root of unity. A zero ω of a simplified $\Phi_h(x^k/n)$ is a zero of

$$x^k-n\zeta_h \tag{2}$$

and hence $R(\omega)$ is an algebraic extension of $R(\zeta_h)$. If the degree of $R(\omega)$ over $R(\zeta_h)$ were k then its degree over R would be $k\varphi(h)$. Hence $\Phi_h(x^k/n)$ is reducible if and only if (2) is reducible over $R(\zeta_h)$. Say

$$x^k-n\zeta_h=F(x)G(x) \qquad F,\, G\in R(\zeta_h)[x]\,. \tag{3}$$

Since all the roots of (2) are of the form $n^{1/k}\zeta_{kh}^s$ we have

Received July 11, 1955.

$$F(0)=n^{l/k}\zeta \in R(\zeta_h) \qquad l=\deg F$$

where ζ is a root of unity. In other words

$$n^{l/k} \in R(\zeta_h, \zeta)=R(\zeta') \tag{4}$$

where ζ' is a root of unity.

According to the lemma (4) is impossible if the reduced fraction $1/k$ has denominator >2. For k odd this means $l=0$ or k and $\Phi_h(x^k/n)$ irreducible. For k even and $0<l<k$ we can have only $l=k/2$. In this case

$$F(0)=\pm n^{1/2}\zeta_{hk}^s , \qquad G(0)=\pm n^{1/2}\zeta_{hk}^t ;$$

and since both $F(0)G(0)$ and $F(0)/G(0)$ are in $R(\zeta_h)$ we obtain

$$s+t\equiv s-t\equiv 0 \pmod{k}.$$

Hence $s\equiv t\equiv 0 \pmod{l}$ so that

$$F(0)=\sqrt{n\zeta_h^u} \in R(\zeta_h). \tag{5}$$

But we noted in [1, Lemma 1] that (5) is necessary and sufficient for the reducibility of $\Phi_h(x^2/n)$. Thus we have

$$\Phi_h(x^2/n)=g(x)g(-x) \text{ and therefore}$$

$$\Phi_h(x^k/n)=g(x^l)g(-x^l)$$

as the complete factorization of $\Phi_h(x^k/n)$ over $R[x]$.

REFERENCES

1. A. J. Hoffman, M. Newman, E. G. Straus, O. Taussky, *The number of absolute points of a correlation*, Pacific J. Math., **6** (1956).
2. K. T. Vahlen, *Über reductible Binome*, Acta. Math., **19** (1895).

UNIVERSITY OF CALIFORNIA, LOS ANGELES
NATIONAL BUREAU OF STANDARDS