104. *Certain Irreducible Polynomials with Multiplicatively Independent Roots*

By Kyoji SAITO

Research Institute for Mathematical Sciences, Kyoto University

(Communicated by Kunihiko KODAIRA, M. J. A., Nov. 12, 1982)

§ 1. **Statement of the results.** For an integer $k \geq 3$, let us define a polynomial $P_{k,p}$ of degree $p \geq 4$:

$$P_{k,p}(x) = x^p + k(x^{p-1} + x^{p-2} + \cdots + x) + 1.$$

In this note, we prove the following theorem.

Theorem. 1. *For even* p, $P_{k,p}(x)$ *is irreducible over* $\boldsymbol{Z}$. *For odd* p, $(x+1)^{-1}P_{k,p}(x)$ *is irreducible over* $\boldsymbol{Z}$.

2. *The polynomial has the following decompositions.*

$$P_{k,p}(x) = (x+\alpha)(x+\alpha^{-1}) \prod_{i=1}^{p/2-1} (x-\varepsilon_i)(x-\bar{\varepsilon}_i) \qquad \textit{for even } p$$

$$= (x+1)(x+\alpha)(x+\alpha^{-1}) \prod_{i=1}^{(p-1)/2-1} (x-\varepsilon_i)(x-\bar{\varepsilon}_i) \qquad \textit{for odd } p$$

where α *is a real number such that* $0 < |\alpha - k + 1| < (k-1)^{-(p-3)}$ *and* $|\varepsilon_i| = 1$, $i = 1, \cdots, [p/2]-1$. *Here* $\bar{\varepsilon}$ *means the complex conjugate of* ε *and* $|\varepsilon| = \sqrt{\varepsilon\bar{\varepsilon}}$.

3. *The roots* $\alpha, \varepsilon_1, \cdots, \varepsilon_{[p/2]-1}$ *in the above expression are multiplicatively independent in* $\boldsymbol{C}^\times = \{\alpha \in \boldsymbol{C} : \alpha \neq 0\}$.

The theorem is proven in [1] § 3 (3.8) 2) for the case $k=3$. Then Prof. G. Fujisaki asked the author whether it is true for $k \geq 3$. In fact it is true as we see in this note. The author would like to express his gratitude to Prof. G. Fujisaki.

§ 2. **A sketch of the proof of the theorem.** For a fixed k, the sequence $P_p = P_{k,p}$, $p \geq 4$ of the polynomials satisfies the following recursion formula.

$$P_{p+2}(x) = (x^2+1)P_p(x) - x^2 P_{p-2}(x) \qquad \text{for } p \geq 4. \tag{2.1}$$

Define new polynomials in $z = x + x^{-1}$ by,

$$(2.2) \qquad Q_q(z) := x^{-q} P_{2q}(x) \qquad q = 2, 3, 4, \cdots$$

$$R_q(z) := (x+1)^{-1} x^{-q} P_{2q+1}(x) \qquad q = 2, 3, 4, \cdots.$$

Then the recursion formula (2.1) turns out to be,

$$(2.3) \qquad Q_{q+1}(z) = zQ_q(z) - Q_{q-1}(z) \qquad q = 2, \cdots$$

$$R_{q+1}(z) = zR_q(z) - R_{q-1}(z) \qquad q = 2, \cdots.$$

Now let us show the following assertion.

Assertion. *The equation* $Q_q(z) = 0$ (resp. $R_q(z) = 0$) *has* q *real simple roots.* $q-1$ *of them lie in the interval* $(-2, 2)$ *and the remaining one lies in the interval* $(-\infty, -2)$.

Furthermore in each connected component of $\boldsymbol{R}$-{roots of $Q_q(z)=0$} (resp. $\boldsymbol{R}$-{roots of $R_q(z)=0$}), *there exists exactly one root of* $Q_{q+1}(z)=0$ (resp. $R_{q+1}(z)=0$).

Proof of the assertion. We prove the assertion only for the sequence $Q_q(z)$, since the other case is shown completely parallel to that case.

We prove the assertion by induction on q, where the statements is trivially true for $q=2$, $Q_2=z^2+kz+k-2$.

Let $\beta_1, \cdots, \beta_q$ be roots of $Q_q(z)=0$ such that $2>\beta_1>\cdots>\beta_{q-1}>-2>\beta_q$. It is enough to show that there exists at least one root of $Q_{q+1}(z)=0$ on each interval $(\beta_1, 2)$, (β_2, β_1), $\cdots$, $(\beta_{q-1}, \beta_{q-2})$, $(-2, \beta_{q-1})$ and $(-\infty, \beta_q)$. By induction hypothesis, $(-1)^{i-1}Q_{q-1}(\beta_i)>0$ for $i=1, \cdots, q$. Then using the recursion (2.3),

$$(2.4)\qquad (-1)^i Q_{q+1}(\beta_i)>0 \qquad \text{for } i=1, \cdots, q.$$

On the other hand, one computes easily

$$(2.5)\qquad Q_{q+1}(2)=2+(2q+1)k>0$$

$$(2.6)\qquad Q_{q+1}(-2)=(-1)^q(k-2)/2^{q+1}$$

$$(2.7)\qquad \lim_{z\to-\infty} Q_{q+1}(z)=(-1)^q\infty.$$

Now looking carefully the change of the sign of the values of the function $Q_{q+1}(z)$, $z\in\boldsymbol{R}$ in (2.4)–(2.7), one proves the assertion.

Proof of 2. A root β of $Q_q(z)$ in the interval $(-2, 2)$ corresponds to two roots $x^2-\beta x+1=0$ of $P_{2p}(x)=0$ with absolute value equal to 1 and a root β of $Q_q(z)$ in the interval $(-\infty, -2)$ corresponds to two minus real roots of $P_{2p}(x)=0$. Hence 2 of the theorem is shown.

Proof of 1. First let us show that if $P_{k,p}(x)$ is reducible to $Q_1(x)Q_2(x)$, then either one of $Q_i(x)$ is a cyclotomic polynomial. First $Q_1(0)Q_2(0)=P_{k,p}(0)=1$. Hence $Q_i(0)=\pm 1$. i.e. $\prod_{\alpha_j;\text{root of } Q_1}|\alpha_j|=1$. Hence in the decomposition of 2, if $-\alpha$ is a root of $Q_1(x)=0$, $-\alpha^{-1}$ should be a root of $Q_1(x)$ also. Then the root of $Q_2(x)=0$ consists only of numbers ε with $|\varepsilon|=1$, which means that $Q_2(x)$ is a cyclotomic polynomial due to a theorem of Kronecker.

Suppose $P_{k,p}(x)$ is reducible and has a root $\exp(2\pi\sqrt{-1}/m)$ for a integer $m>2$. Using an expression

$$P_{k,p}(x)=(x-1)^{-1}\{x^{p+1}-1+(k-1)(x^p-x)\}$$

one obtains,

$$P_{k,p}(e^{\sqrt{-1}2\pi/m})=\frac{\exp(\sqrt{-1}p\pi/m)}{\sin(\pi/m)} \times\{\sin((p+1)\pi/m)+(k-1)\sin((p-1)\pi/m)\}.$$

Put $p=tm+r$ for some integers t, r with $0\leq r<m$. One may assume $r\neq 0$. Then in the above expression two terms $\sin((p+1)\pi/m)=(-1)^t\sin((r+1)\pi/m)$, $\sin((p-1)\pi/m)=(-1)^t\sin((r-1)\pi/m)$ have the same sign $(-1)^t$, so that sum becomes zero iff $(r+1)/m$, $(r-1)/m\in\boldsymbol{Z}$,

which implies $m=2$, $r=1$.

Proof of 3. Suppose that there exist integers $m, m_1, \cdots, m_{[p/2]-1}$, such that $\alpha^m \prod_j \varepsilon_j^{m_j} = \pm 1$. By taking the absolute values of both sides $\alpha^m=1$. Hence $m=1$. Consider the action of the Galois group of the splitting field of $P_{k,p}=0$ over $\boldsymbol{Q}$ on the roots of $P_{k,p}=0$. Since $P_{k,p}$ is irreducible there exists an element σ of the Galois group such that $\sigma\varepsilon_1 = -\alpha$ and σ induces a permutation of $\varepsilon_2^{\pm 1}, \cdots, \varepsilon_{[p/2]-1}^{\pm 1}$ to some of $\varepsilon_1^{\pm 1}, \cdots, \varepsilon_{[p/2]-1}^{\pm 1}$. Applying σ on the relation $\prod_j \varepsilon_j^{m_j} = \pm 1$, one gets $\alpha^{m_1} \prod_{j\geq 2} \sigma(\varepsilon_j)^{m_j} = \pm 1$. Again taking the absolute values of both sides, one get $m_1=0$. Repeating this process, one proves $m=m_1=m_2=\cdots=m_{[p/2]-1}=0$.

This completes the proof of the theorem.

Reference

[1] K. Saito: The zeroes of characteristic function χ_f for the exponents of a hypersurface isolated singular point. Advanced Studies in Pure Mathematics, 1, 193–215 (1982).