KMITL Sci. Tech. J. Vol. 17 No. 1 Jan.-Jun. 2017

Polynomial Whose Values at the Integers are n-th Power of Integers in a Quadratic Field

Janyarak Tongsomporn[1*] and Vichian Laohakosol[2]

[1] School of Science, Walailak University, Nakhon Si Thammarat, Thailand
[2] Department of Mathematics, Faculty of Science, Kasetsart University, Bangkok, Thailand

Abstract

Let $f(x_1, x_2, \ldots, x_k) \in \mathcal{K}[x_1, x_2, \ldots, x_k]$, where $\mathcal{K}$ is a quadratic field. We investigate the polynomial $f(x_1, x_2, \ldots, x_k)$ which becomes always an n^{th} power of an quadratic integer using the technique of Kojima. It is shown that if $f(\alpha_1, \alpha_2, \ldots, \alpha_k)$ is an n^{th} power of an element in $O_{\mathcal{K}}$, the ring of integers of $\mathcal{K}$, then $f(x_1, x_2, \ldots, x_k) = (\phi(x_1, x_2, \ldots, x_k))^n$,for some $\phi(x_1, x_2, \ldots, x_k) \in O_K[x_1, x_2, \ldots, x_k]$.

Keywords: integer-valued polynomial, quadratic integer.

1. Introduction

In 1912, Jentzsch [1] proposed the following problem.

If a polynomial $f(x)$ with integral coefficients is a square of an integer for any integral value of x, then $f(x)$ is a square of a polynomial with integral coefficients.

Grösch solved it in 1913 and later in 1915, Kojima [1, Theorem 6', p. 32] extended it to the following theorem.

Let $f(x_1, x_2, \ldots, x_k)$ be a polynomial in $x_1, x_2, \ldots, x_k$ with integral coefficients. If for any integral values of $x_1, x_2, \ldots, x_k$ it becomes always power of an integer, n being a positive integer, then $f(x_1, x_2, \ldots, x_k)$ has the form $\varphi(x_1, x_2, \ldots, x_k)^n$, where φ is a polynomial with integral coefficients.

In 1950, Fuchs [2] proved the following much more general result.

If $f(x)$ and $g(x)$ are polynomials and if for every integer $p > p_0$, there is an integer $q = g(p) > 0$ such that $f(p) = g(q)$, then $f(x) = g(h(x))$, where $h(x)$ is a polynomial. If $f(x)$ and $g(x)$ have integral coefficients and $g(x)$ has leading coefficient 1, then $h(x)$ also has integral coefficients. Later in 1957, Shapiro [3] gave a simple proof of the following generalization.

Let $P(x)$ and $Q(x)$ be polynomials which are integer-valued at the integers, of degrees p and q, respectively. If $P(n)$ is of the form $Q(m)$ for all n , or even for in finitely many blocks of consecutive integers of length $\geq \frac{p}{q} + 2$,then there is a polynomial $R(x)$ such that $P(x) = Q(R(x))$

*Corresponding author: E-mail: janyarak.to@wu.ac.th

Motivated by these results, it is natural to ask whether the same result holds for polynomials, of several variables, over a quadratic number field. We give here an affirmative answer using the technique of Kojima [1].

2. Preliminaries

Let $\mathcal{K}(\subset\mathbb{C})$ be a quadratic number field, with $O_{\mathcal{K}}$ as its ring of integers. We start with a few important lemmas.

Lemma 2.1 *If a polynomial* $P(x_1,x_2,\ldots,x_k)\in\mathbb{C}[x_1,x_2,\ldots,x_k]$ *vanishes when we substitute in it*

any one of the elements $\alpha_{1,1},\alpha_{1,2},\ldots,\alpha_{1,m_1+1}$ *for* x_1,

any one of the elements $\alpha_{2,1},\alpha_{2,2},\ldots,\alpha_{2,m_2+1}$ *for* x_2,

$\vdots$

and any one of the elements $\alpha_{k,1},\alpha_{k,2},\ldots,\alpha_{k,m_k+1}$ *for* x_k,

where the $\alpha_{i,j}$ *'s are complex constants subject to the conditions*

$$\alpha_{i,j}\neq\alpha_{i,h}\ \text{, when } j\neq h\text{, for all } i=1,2,\ldots,k,$$

and $m_i\in\mathbb{Z}$ *satisfying* $m_i\geq\deg_{x_i}P\ (i=1,\ldots,k)$, *then* $P(x_1,\ldots,x_k)\equiv 0.$

Proof. The case $k=1$ is trivial since a polynomial of degree m has $m+1$ roots. Assume the result holds for a polynomial in $k-1$ variables. Writing $P(x_1,x_2,\ldots,x_k)$ in the descending powers of x_1 as

$$P(x_1,x_2,\ldots,x_k)=A_0(x_2,\ldots,x_k)x_1^{m_1}+A_1(x_2,\ldots,x_k)x_1^{m_1-1}+\cdots+A_{m_1}(x_2,\ldots,x_k),$$

and substituting each of $x_2,\ldots,x_k$ by any one of their assigned values, the resulting polynomial in x_1 must be zero for m_1+1 different values of x_1. Hence,

$$A_0(\alpha_{2,h_2},\ldots,\alpha_{k,h_k})=0,\ A_1(\alpha_{2,h_2},\ldots,\alpha_{k,h_k})=0,\ldots,A_{m_1}(\alpha_{2,h_2},\ldots,\alpha_{k,h_k})=0,$$

where $h_i=1,2,\ldots,m_i+1$ and $i=2,3,\ldots,k.$ From the induction hypothesis, we have

$$A_0(x_2,\ldots,x_k)\equiv 0, A_1(x_2,\ldots,x_k)\equiv 0,\ldots,A_{m_1}(x_2,\ldots,x_k)\equiv 0,$$

And consequently, $P(x_1,x_2,\ldots,x_k)\equiv 0$.

Lemma 2.2 *Let* $P(x_1,x_2,\ldots,x_k)\in\mathbb{C}[x_1,x_2,\ldots,x_k]$. *If* $P(\alpha_1,\ldots,\alpha_k)\in\mathcal{K}$ *for any* $\alpha_1,\ldots,\alpha_k\in\mathcal{K}$, *then the coefficients of* $P(x_1,x_2,\ldots,x_k)$ *are all in* $\mathcal{K}$.

Proof. For case $k=1$, suppose that $P(x):=a_0x^m+a_1x^{m-1}+\cdots+a_m\in\mathbb{C}[x]$. Substituting distinct values $\alpha_1,\ldots,\alpha_{m+1}\in\mathcal{K}$, we obtain

$$a_0\alpha_1^m+a_1\alpha_1^{m-1}+\cdots+a_{m-1}\alpha_1+a_m=P(\alpha_1)\in\mathcal{K},$$
$$\vdots$$
$$a_0\alpha_{m+1}^m+a_1\alpha_{m+1}^{m-1}+\cdots+a_{m-1}\alpha_{m+1}+a_m=P(\alpha_{m+1})\in\mathcal{K}.$$

Since the coefficient matrix of this linear system

$$\begin{bmatrix} \alpha_1^m & \alpha_1^{m-1} & \cdots & \alpha_1 & 1 \\ \alpha_2^m & \alpha_2^{m-1} & \cdots & \alpha_2 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_{m+1}^m & \alpha_{m+1}^{m-1} & \cdots & \alpha_{m+1} & 1 \end{bmatrix}$$

is a nonzero Vandermonde matrix, solving the system, we see that all $a_i \in \mathcal{K}$.

Assume now that the statement holds for a polynomial in $k-1$ variables. Let P be a polynomial in $x_1, x_2, \ldots, x_k$ and degree of m_1 in x_1. Let

$$P(x_1, x_2, \ldots, x_k) = A_0(x_2, \ldots, x_k)x_1^{m_1} + A_1(x_2, \ldots, x_k)x_1^{m_1-1} + \cdots + A_{m_1}(x_2, \ldots, x_k),$$

For $\alpha_2, \ldots, \alpha_k \in \mathcal{K}$, let $Q(x_1) := P(x_1, \alpha_2, \ldots, \alpha_k) \in \mathbb{C}[x_1]$. By case $k = 1$, we obtain $Q(x_1) \in \mathcal{K}[x_1]$, which implies that

$$A_i(\alpha_2, \ldots, \alpha_k) \in \mathcal{K}\ (i = 0, 1, \ldots, m_1).$$

This holds for any $\alpha_2, \ldots, \alpha_k \in \mathcal{K}$.By the induction hypothesis, all $A_i(x_2, \ldots, x_k) \in \mathcal{K}[x_2, \ldots, x_k]$, showing that $P(x_1, x_2, \ldots, x_k) \in \mathcal{K}[x_1, x_2, \ldots, x_k]$.

We shall also need Hilbert's irreducibility theorem [4, Theorem 33,p. 179] whose convenient form is:

Theorem 2.3 *Let $\mathcal{K}$ be a algebraic number field with ring of integers $O_{\mathcal{K}}$, and let $f(x_1, \ldots, x_r, y)$ be an irreducible polynomial in $\mathcal{K}[x_1, \ldots, x_r, y]$. Then there exists an infinite number of specializations of variables $x_1, \ldots, x_r$ to $a_1, \ldots, a_r \in O_{\mathcal{K}}$ such that $f(a_1, \ldots, a_r, y)$ is an irreducible polynomial in $\mathcal{K}[y]$.*

Another essential theorem is a version of Gauss's lemma for a number field, [5], Theorem 8.6 and Remark 8.7].

Theorem 2.4 *Let $\mathcal{K}$ be a algebraic number field with ring of integers $O_{\mathcal{K}}$ and let $f(x) \in O_{\mathcal{K}}[x]$. If $f(x) = g(x)h(x)$ for polynomials $g(x)$ and $h(x)$ in $\mathcal{K}[x]$ then $g(x)$ and $h(x)$ are in $O_{\mathcal{K}}[x]$.*

3. Results

Theorem 3.1 *Let $a(x_1, x_2, \ldots, x_k)$ be a branch of an algebraic function in $x_1, x_2, \ldots, x_k$ defined by an equation*

$$f(y \mid x_1, x_2, \ldots, x_k) = A_0(x_1, x_2, \ldots, x_k)y^n + A_1(x_1, x_2, \ldots, x_k)y^{n-1} + \cdots + A_n(x_1, x_2, \ldots, x_k) = 0,$$

where $A_0, A_1, A_2, \ldots, A_n \in \mathbb{C}[x_1, x_2, \ldots, x_k]$ are all polynomials having no common factor and n is the chosen least degree in y (i.e., $f(y \mid x_1, x_2, \ldots, x_k)$ considered as a polynomial in y over $\mathbb{C}[x_1, x_2, \ldots, x_k]$ is irreducible over $\mathbb{C}[x_1, x_2, \ldots, x_k]$.)

If $a(x_1, x_2, \ldots, x_k)$ has one and the same value, when we substitute in it *any one of the elements* $\alpha_{1,1},\alpha_{1,2},\ldots,\alpha_{1,m_1+1}$ *for* x_1,

$\vdots$

any one of the elements $\alpha_{k,1},\alpha_{k,2},\ldots,\alpha_{k,m_k+1}$ *for* x_k ,

where the $\alpha_{i,j}$ *'s are complex constant subject to the conditions*

$$\alpha_{i,j}\neq\alpha_{i,h}\quad\left(j\neq h, i=1,2,\ldots,k\right),$$

and $m_i\in\mathbb{Z}$ *satisfying* $m_i\geq\deg_{x_i}P\ (i=1,\ldots,k)$, *then the algebraic function* $a(x_1,x_2,\ldots,x_k)$ *must be constant.*

Proof. Let c be the value of $a(x_1,x_2,\ldots,x_k)$ when we substitute the assigned values for $x_1,x_2,\ldots,x_k$. Then $f(c\mid x_1,x_2,\ldots,x_k)$ is the polynomial in $x_1,x_2,\ldots,x_k$ and vanishes for any one set of the assigned values of $x_1,x_2,\ldots,x_k$. By Lemma2.1, $f(c\mid x_1,x_2,\ldots,x_k)\equiv 0$. Consider

$$F(y):=A_0\left(x_1,x_2,\ldots,x_k\right)y^n+A_1\left(x_1,x_2,\ldots,x_k\right)y^{n-1}+\cdots+A_n\left(x_1,x_2,\ldots,x_k\right).$$

Since $F\left(c\right)=0,$ we have $\left(y-c\right)\mid F\left(y\right),$ which contradicts its irreducibility unless $n=1$. Hence,

$$f(y\mid x_1,x_2,\ldots,x_k)=F(y)=\alpha(y-c),$$

where $\alpha\in\mathbb{C}$. Thus, $a(x_1,x_2,\ldots,x_k)\equiv c$.

Combining Theorem 3.1 with the above lemmas, we get

Theorem 3.2 *If a branch of an algebraic function* $a(x_1,x_2,\ldots,x_k)$ *takes a value in* $\mathcal{K}$ *when we substitute* $x_1,x_2,\ldots,x_k$ *by elements in* $\mathcal{K}$ *,then the numerical coefficients in* $f(y\mid x_1,x_2,\ldots,x_k)$ *are in* $\mathcal{K}$ *.*

Proof. First, we prove the theorem for an algebraic function of a single variable. Let $a(x)$ be such a branch of an algebraic function defined by

$$f(y\mid x)=A_0\left(x\right)y^n+A_1\left(x\right)y^{n-1}+\cdots+A_{n-1}\left(x\right)y+A_n\left(x\right)=0, \tag{3.1}$$

where

$$A_i(x)=a_{i,0}x^{m_i}+a_{i,1}x^{m_i-1}+\ldots+a_{i,m_i-1}x+a_{i,m_i}\ (i=0,1,\ldots,n),\ a_{0,0}=1,$$

and all $A_i(x)$'s have no common factor. Then

$$\#\left\{a_{i,k};\,a_{i,k}\neq a_{0,0}\right\}=m_0+(m_1+1)+(m_2+1)+\cdots+(m_n+1)=m_0+m_1+m_2+\cdots+m_n+n$$
$$:=m.$$

Let $c_1,c_2,\ldots,c_m$ be any m distinct elements in $\mathcal{K}$. Then $y_i:=a(c_i)\in\mathcal{K}\ (i=1,2,\ldots,m)$. Thus we have the system of linear equations with regard to $a_{i,k}$, whose coefficients are all quadratic numbers,

$$
\begin{aligned}
0 &= A_0(c_1)y_1^n + A_1(c_1)y_1^{n-1} + \cdots + A_{n-1}(c_1)y_1 + A_n(c_1) \\
&= \left(c_1^{m_0} + a_{0,1}c_1^{m_0-1} + \ldots + a_{0,m_0-1}c_1 + a_{0,m_0}\right)y_1^n \\
&\quad + \left(a_{1,0}c_1^{m_1} + a_{1,1}c_1^{m_1-1} + \ldots + a_{1,m_1-1}c_1 + a_{1,m_1}\right)y_1^{n-1} + \cdots \\
&\quad + \left(a_{n,0}c_1^{m_n} + a_{n,1}c_1^{m_n-1} + \ldots + a_{n,m_n-1}c_1 + a_{n,m_n}\right) \\
&\ \vdots \\
0 &= A_0(c_m)y_m^n + A_1(c_m)y_m^{n-1} + \cdots + A_{n-1}(c_m)y_m + A_n(c_m) \\
&= \left(c_m^{m_0} + a_{0,1}c_m^{m_0-1} + \ldots + a_{0,m_0-1}c_m + a_{0,m_0}\right)y_m^n \\
&\quad + \left(a_{1,0}c_m^{m_1} + a_{1,1}c_m^{m_1-1} + \ldots + a_{1,m_1-1}c_m + a_{1,m_1}\right)y_m^{n-1} + \cdots \\
&\quad + \left(a_{n,0}c_m^{m_n} + a_{n,1}c_m^{m_n-1} + \ldots + a_{n,m_n-1}c_m + a_{n,m_n}\right).
\end{aligned}
$$

We claim that the elements $c_1, c_2, \ldots, c_m$ can be chosen so that the determinant of this system does not vanish. For otherwise, for any $c_1, c_2, \ldots, c_m \in \mathcal{K}$, the determinant

$$
\varphi_1(c_1, y_1; c_2, y_2; \ldots; c_m, y_m) := \begin{vmatrix}
c_1^{m_0-1}y_1^n & \ldots & y_1^n & c_1^{m_1}y_1^{n-1} & \ldots & y_1^{n-1} & \cdots & c_1^{m_n} & \ldots & 1 \\
c_2^{m_0-1}y_2^n & \ldots & y_2^n & c_2^{m_1}y_2^{n-1} & \ldots & y_2^{n-1} & \cdots & c_2^{m_n} & \ldots & 1 \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \cdots & \vdots & \ddots & \vdots \\
c_m^{m_0-1}y_m^n & \ldots & y_m^n & c_m^{m_1}y_m^{n-1} & \ldots & y_m^{n-1} & \cdots & c_m^{m_n} & \ldots & 1
\end{vmatrix}
$$

vanishes. Considering $c_2, c_3, \ldots, c_m$, and consequently $y_2, y_3, \ldots, y_m$ as constants, it follows from our assumption that $a(x)$ is an algebraic function in x defined by $\varphi_1(x, a(x); c_2, y_2; \ldots; c_m, y_m) = 0$ which vanishes for any $x \in \mathcal{K}$. By Theorem 3.1,

$$
\varphi_1(x, a(x); c_2, y_2; \ldots; c_m, y_m) \equiv 0.
$$

If $\varphi_1(x, y; c_2, y_2; \ldots; c_m, y_m)$ considered as a polynomial in x and y does not vanish identically, the equation $\varphi_1(x, y; c_2, y_2; \ldots; c_m, y_m) = 0$ in y has a common root with the equation (3.1); but since the degree of the equation $\varphi_1 = 0$ is not greater than n, and the degree with respect to x of the coefficient of y^n is less than that of (3.1), we must have $\varphi_1(x, y; c_2, y_2; \ldots; c_m, y_m) \equiv 0$, and consequently the first principal minor of the determinant, i.e.,

$$
\varphi_2(c_2, y_2; \ldots; c_m, y_m) := \begin{vmatrix}
c_2^{m_0-2}y_2^n & \ldots & y_2^n & c_2^{m_1}y_2^{n-1} & \ldots & y_2^{n-1} & \cdots & c_2^{m_n} & \ldots & 1 \\
c_3^{m_0-2}y_3^n & \ldots & y_3^n & c_3^{m_1}y_3^{n-1} & \ldots & y_3^{n-1} & \cdots & c_3^{m_n} & \ldots & 1 \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \cdots & \vdots & \ddots & \vdots \\
c_m^{m_0-2}y_m^n & \ldots & y_m^n & c_m^{m_1}y_m^{n-1} & \ldots & y_m^{n-1} & \cdots & c_m^{m_n} & \ldots & 1
\end{vmatrix}
$$

vanishes identically. In this expression, since the elements $c_2, c_3, \ldots, c_m \in \mathcal{K}$ are arbitrary, by the same reasoning as above, we have $\varphi_2(x, y; c_3, y_3; \ldots; c_m, y_m) \equiv 0$, so the second principal minor, i.e.,

$$\begin{vmatrix} c_3^{m_0-3}y_3^n & \dots & y_3^n & c_3^{m_1}y_3^{n-1} & \dots & y_3^{n-1} & \cdots & c_3^{m_n} & \dots & 1 \\ c_4^{m_0-3}y_4^n & \dots & y_4^n & c_4^{m_1}y_4^{n-1} & \dots & y_4^{n-1} & \cdots & c_4^{m_n} & \dots & 1 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ c_m^{m_0-3}y_m^n & \dots & y_m^n & c_m^{m_1}y_m^{n-1} & \cdots & y_m^{n-1} & \cdots & c_m^{m_n} & \dots & 1 \end{vmatrix}$$

vanishes identically. Repeating this process, we arrive at

$$\begin{vmatrix} c_{m-m_n+1}^{m_n} & c_{m-m_n+1}^{m_n-1} & \dots & c_{m-m_n+1} & 1 \\ c_{m-m_n+2}^{m_n} & c_{m-m_n+2}^{m_n-1} & \dots & c_{m-m_n+2} & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_m^{m_n} & c_m^{m_n-1} & \dots & c_m & 1 \end{vmatrix} \equiv 0,$$

Which is a contradiction for distinct c_i's, showing that Theorem 3.2 is true for an algebraic function of a single variable. Next, we prove the theorem for an algebraic function of several variables. Let $a(x_1, x_2, \dots, x_k)$ be a branch of the algebraic function defined by

$$f(y \mid x_1, x_2, \dots, x_k) = A_0(x_1, x_2, \dots, x_k)y^n + A_1(x_1, x_2, \dots, x_k)y^{n-1} + \cdots + A_n(x_1, x_2, \dots, x_k) = 0, \quad (3.2)$$

where

$$A_i(x_1, x_2, \dots, x_k) = B_{i,0}(x_2, \dots, x_k)x_1^{m_i} + \cdots + B_{i,m_i}(x_2, \dots, x_k) \quad (i = 0,1,2,\dots,n),$$

Where $B_{i,h}$ $(h = 0,1,2,\dots,m_i)$ are polynomials in $x_2, \dots, x_k$. Substituting any elements $\overline{c_2}, \dots, \overline{c_k}$ in $\mathcal{K}$ for $x_2, \dots, x_k$, respectively, into the equation (3.2), we see that for every element of $x_1 \in \mathcal{K}$, the equation

$$A_0(x_1, \overline{c_2}, \dots, \overline{c_k})y^n + A_1(x_1, \overline{c_2}, \dots, \overline{c_k})y^{n-1} + \cdots + A_n(x_1, \overline{c_2}, \dots, \overline{c_k}) = 0$$

must be satisfied by the corresponding element of $y = a(x_1, \overline{c_2}, \dots, \overline{c_k})$, which implies that $B_{i,h}(\overline{c_2}, \dots, \overline{c_k}) \in \mathcal{K}$. By Lemma3.2, all the numerical coefficients of the equation (3.2) are in $\mathcal{K}$.

Pushing further, we have the following:

Theorem 3.3 *If a branch of an algebraic function* $a(x_1, x_2, \dots, x_k)$ *takes values in* $O_{\mathcal{K}}$ *for any* $x_1, x_2, \dots, x_k$ *in* $O_{\mathcal{K}}$*, then it is a polynomial with coefficients in* $\mathcal{K}$.

Proof. Let $a(x_1, x_2, \dots, x_k)$ be a branch of an algebraic function defined by

$$f(y \mid x_1, x_2, \dots, x_k) = A_0(x_1, x_2, \dots, x_k)y^n + A_1(x_1, x_2, \dots, x_k)y^{n-1} + \cdots + A_n(x_1, x_2, \dots, x_k) = 0,$$

where $A_i(x_1, x_2, \dots, x_k) \in \mathcal{K}[x_1, x_2, \dots, x_k]$ $(i = 0,1,\dots,n)$. Suppose that $n > 1$. If we substitute any $c_1, c_2, \dots, c_k$ in $\mathcal{K}$ for $x_1, x_2, \dots, x_k$, then $f(y \mid c_1, c_2, \dots, c_k)$ is reducible in $\mathcal{K}[y]$; hence, by Hilbert's irreducibility Theorem 2.3, $f(y \mid x_1, x_2, \dots, x_k)$ is reducible,
which is a contradiction. Thus, $n = 1$, i.e.,

$$f(y \mid x_1, x_2, \dots, x_k) = A_0(x_1, x_2, \dots, x_k)y + A_1(x_1, x_2, \dots, x_k) = 0,$$

yielding

$$y(x_1,x_2,\dots,x_k) = -\frac{A_1(x_1,x_2,\dots,x_k)}{A_0(x_1,x_2,\dots,x_k)} = q(x_1 \mid x_2,\dots,x_k) + \frac{r(x_1 \mid x_2,\dots,x_k)}{A_0(x_1 \mid x_2,\dots,x_k)},$$

where q,r are polynomials in x_1 whose coefficients are rational functions of $x_2,\dots,x_k$ with coefficients in $\mathcal{K}$, such that $\deg_{x_1} r < \deg_{x_1} A_0$. Thus, we can represent y in the form

$$y = \frac{Q(x_1 \mid x_2,\dots,x_k)}{L(x_2,\dots,x_k)} + \frac{C_0(x_2,\dots,x_k)x_1^{m_0-1} + C_1(x_2,\dots,x_k)x_1^{m_0-2} + \dots + C_{m_0-1}(x_2,\dots,x_k)}{B_0(x_2,\dots,x_k)x_1^{m_0} + B_1(x_2,\dots,x_k)x_1^{m_0-1} + \dots + B_{m_0}(x_2,\dots,x_k)}, \quad (3.3)$$

where $Q(x_1 \mid x_2,\dots,x_k)$ is a polynomial in x_1 whose coefficients are polynomials in $O_{\mathcal{K}}[x_2,\dots,x_k]$, and $L(x_2,\dots,x_k) \in O_{\mathcal{K}}[x_2,x_3,\dots,x_k]$ is the least common multiple of the denominators of coefficients in $q(x_1 \mid x_2,\dots,x_k)$, and all C 's and B's are the polynomials in $\mathcal{K}[x_2,x_3,\dots,x_k]$. Let

$$m_i = \max_{0 \le j \le m_0-1}\left\{\deg_{x_i} C_j\right\} \quad (i = 2,3,\dots,k).$$

Choose a system of elements $\alpha_{i,h} \in O_{\mathcal{K}} \quad (h = 1,2,\dots,m_i+1; i = 1,2,\dots,k)$ with

$$\alpha_{i,j} \ne \alpha_{i,h} \quad (j \ne h, i = 1,2,\dots,k),$$

such that when we substitute in (3.3)

any one of the elements $\alpha_{2,1},\alpha_{2,2},\dots,\alpha_{2,m_2+1} \in O_{\mathcal{K}}$ for x_2 ,

$\vdots$

any one of the elements $\alpha_{k,1},\alpha_{k,2},\dots,\alpha_{k,m_k+1} \in O_{\mathcal{K}}$ for x_k ,

neither the polynomial $L(x_2,\dots,x_k)$ nor $B_i(x_2,\dots,x_k)$ vanishes. Since

$$y(x_2,\dots,x_k)L(x_2,\dots,x_k) - Q(x_1 \mid x_2,\dots,x_k) \quad (3.4)$$

$$= \frac{C_0(x_2,\dots,x_k)x_1^{m_0-1} + C_1(x_2,\dots,x_k)x_1^{m_0-2} + \dots + C_{m_0-1}(x_2,\dots,x_k)}{B_0(x_2,\dots,x_k)x_1^{m_0} + B_1(x_2,\dots,x_k)x_1^{m_0-1} + \dots + B_{m_0}(x_2,\dots,x_k)} L(x_2,\dots,x_k),$$

when we substitute the above assigned values of $x_2,\dots,x_k$ into (3.4), the left hand side of (3.4) is in $O_{\mathcal{K}}$ for any $x_1 \in O_{\mathcal{K}}$. But we can choose $x_1 \in O_{\mathcal{K}}$ such that the right hand side of (3.4) is not in $O_{\mathcal{K}}$. Thus, $C_i(x_2,\dots,x_k)$ must vanish for the above assigned values of $x_2,\dots,x_k$ for all $i = 0,1,\dots,m_0-1$. By Lemma 2.1 , $C_i(x_2,\dots,x_k) \equiv 0 \;\; (i = 0,1,\dots,m_0-1)$, i.e.,

$$y(x_1,x_2,\dots,x_k) = \frac{Q(x_1 \mid x_2,\dots,x_k)}{L(x_2,\dots,x_k)} \in \mathcal{K}(x_2,\dots,x_k)[x_1].$$

Proceeding in the same manner, we have

$$y(x_1,x_2,\dots,x_k) \in \mathcal{K}(x_1,x_3,\dots,x_k)[x_2], \dots, y(x_1,x_2,\dots,x_k) \in \mathcal{K}(x_1,x_2,\dots,x_{k-1})[x_k].$$

Therefore, $y(x_1,x_2,\dots,x_k) \in \mathcal{K}[x_1,x_2,\dots,x_k]$.

In the proof of Theorem 3.3 the following result is implicit.

Theorem 3.4 *If a branch of an algebraic function takes valuein $\mathcal{K}$ for any $x_1,x_2,\dots,x_k$ in $O_{\mathcal{K}}$, then it is a rational function in $x_1,x_2,\dots,x_k$ with coefficients in $\mathcal{K}$.*

We are now ready to state and prove our first main result.

Theorem 3.5 *Let* $n \in \mathbb{N}$. *If* $f(x_1, x_2, \ldots, x_k)$ *is an algebraic function of* $x_1, x_2, \ldots, x_k$ *taking values which are* n^{th} *powers of elements in* $O_{\mathcal{K}}$ *when we substitute for* $x_1, x_2, \ldots, x_k$ *by elements in* $O_{\mathcal{K}}$ *then*

$$f(x_1, x_2, \ldots, x_k) = \phi(x_1, x_2, \ldots, x_k)^n,$$

for some $\phi(x_1, x_2, \ldots, x_k) \in \mathcal{K}[x_1, x_2, \ldots, x_k]$.

Proof. Since $\sqrt[n]{f(x_1, x_2, \ldots, x_k)}$ is a branch of an algebraic function, and $\sqrt[n]{f(c_1, c_2, \ldots, c_k)} \in O_{\mathcal{K}}$ for all $c_i \in O_{\mathcal{K}}$ $(i = 1, 2, \ldots, k)$, by Theorem 3.3, $\sqrt[n]{f(x_1, x_2, \ldots, x_k)}$ is a polynomial in $x_1, x_2, \ldots, x_k$ with coefficients in $\mathcal{K}$.

For polynomials, we now prove the following:

Corollary 3.6 *Let* $f(x_1, x_2, \ldots, x_k) \in O_{\mathcal{K}}[x_1, x_2, \ldots, x_k]$ *and let* $n \in \mathbb{N}$. *If* $f(\alpha_1, \ldots, \alpha_k)$ *is an* n^{th} *power of an element in* $O_{\mathcal{K}}$ *for any* $\alpha_1, \ldots, \alpha_k$ *in* $O_{\mathcal{K}}$ *then* $f(x_1, x_2, \ldots, x_k) = \phi(x_1, x_2, \ldots, x_k)^n$ *for some* $\phi \in O_{\mathcal{K}}[x_1, x_2, \ldots, x_k]$.

Proof. From Theorem 3.5 , we know that $f(x_1, x_2, \ldots, x_k) = \phi(x_1, x_2, \ldots, x_k)^n$, for some $\phi(x_1, x_2, \ldots, x_k) \in \mathcal{K}[x_1, x_2, \ldots, x_k]$. It remains to show that indeed $\phi(x_1, x_2, \ldots, x_k) \in O_{\mathcal{K}}[x_1, x_2, \ldots, x_k]$. Let

$$\phi\left(x_1, x_2, \ldots, x_k\right) = \sum_{\underline{i} = (i_1, \ldots, i_k)} \frac{\alpha'(\underline{i})}{\beta(\underline{i})} x_1^{i_1} x_2^{i_2} \cdots x_k^{i_k} \tag{3.5}$$

where $\alpha'(\underline{i}), \beta(\underline{i}) (\neq 0)$ are relatively prime integers in $O_{\mathcal{K}}$. We may assume that the monomials appearing in the right-hand expression of (3.5) are written in ascending lexicographical order, i.e.,

$$x_1^{j_1} x_2^{j_2} \cdots x_k^{j_k} \prec x_1^{i_1} x_2^{i_2} \cdots x_k^{i_k}$$

if any of the following conditions hold: $i_1 > j_1$; or $i_1 = j_1$ but $i_2 > j_2$; or generally, $i_1 = j_1, \ldots, i_{\ell-1} = j_{\ell-1}$ but $i_\ell > j_\ell$ for some $\ell \le k$. Let

$$L := \operatorname{lcm}_{\underline{i}} \{\beta(\underline{i})\}, \ g := \gcd_{\underline{i}} \{\alpha'(\underline{i})\}, \alpha(\underline{i}) := \frac{\alpha'(\underline{i})}{g},$$

So that $\gcd_{\underline{i}} \{\alpha(\underline{i})\} = 1$. Thus,

$$L^n f(x_1, x_2, \ldots, x_k) = g^n \left(\sum_{\underline{i}} \frac{L\alpha(\underline{i})}{\beta(\underline{i})} x_1^{i_1} x_2^{i_2} \cdots x_k^{i_k} \right)^n \in O_{\mathcal{K}}[x_1, x_2, \ldots, x_k]. \tag{3.6}$$

If L is not a unit, let π be its prime factor.

We claim that π divides all $L\alpha(\underline{i}) / \beta(\underline{i})$. If not, then let $\underline{I} = (I_1, I_2, \ldots, I_k)$ be the least (lexicographically) index for which $\pi \mid L\alpha(\underline{i}) / \beta(\underline{i})$ with $\underline{i} \prec \underline{I}$ but $\pi \nmid L\alpha(\underline{I}) / \beta(\underline{I})$. Observe then that in the expression on the right-hand side of (3.6) , the integer coefficient of

$\left(x_1^{I_1}x_2^{I_2}\cdots x_k^{I_k}\right)^n$ is not divisible by π, as it contains a single term $(gL\alpha(\underline{I})/\beta(\underline{I}))^n$ not divisible by π, which contradicts the fact that all coefficients on the left-hand side are divisible π . Thus, π must divide all coefficients in the right-hand expression, but this in turn implies then that L is not the least common multiple of the denominators $\beta(\underline{i})$. This contradiction shows that L must be a unit, i.e., all $\beta(\underline{i})$ are units.

Remark. There is another proof of Corollary 3.6 using Theorem 2.4 (Gauss's lemma) for the case $k=1$. From Theorem 3.5 , we know that $f(x)=\phi(x)^n$, for some $\phi(x)\in\mathcal{K}[x]$. By Theorem 2.4, $\phi(x)\in O_{\mathcal{K}}[x]$.

4. Acknowledgements

The first author is supported by the Institute of Research and Development, Walailak university. The second author is supported by the Center for Advanced Studies in Industrial Technology and the Faculty of Science, Kasetsart University.

References

[1] Kojima, T., **1915**. Note on number-theoretical properties of algebraic functions. *Tohoku Math. J.*, 8, 24-27.

[2] Fuchs, W.H.J., **1950**. A polynomial the square of another polynomial. *Amer. Math. Monthly*, 57, 114-116.

[3] Shapiro, H.S., **1957**. The range of an integer-valued polynomial. *Amer. Math. Monthly*, 64, 424-425.

[4] Schinzel, A., **1982**. Selected Topics on Polynomials. University of Michigan Press.

[5] Magidin, A., McKinnon, D., **2005**. Gauss's lemma for number fields. *Amer. Math. Monthly*, 112(5), 385-416.