Korean J. Math. **30** (2022), No. 3, pp. 425–431
http://dx.doi.org/10.11568/kjm.2022.30.3.425

FACTORIZATION IN THE RING $h(\mathbb{Z}, \mathbb{Q})$ OF COMPOSITE HURWITZ POLYNOMIALS

Dong Yeol Oh† and Ill Mok Oh

Abstract. Let $\mathbb{Z}$ and $\mathbb{Q}$ be the ring of integers and the field of rational numbers, respectively. Let $h(\mathbb{Z}, \mathbb{Q})$ be the ring of composite Hurwitz polynomials. In this paper, we study the factorization of composite Hurwitz polynomials in $h(\mathbb{Z}, \mathbb{Q})$. We show that every nonzero nonunit element of $h(\mathbb{Z}, \mathbb{Q})$ is a finite $*$-product of quasi-primary elements and irreducible elements of $h(\mathbb{Z}, \mathbb{Q})$. By using a relation between usual polynomials in $\mathbb{Q}[x]$ and composite Hurwitz polynomials in $h(\mathbb{Z}, \mathbb{Q})$, we also give a necessary and sufficient condition for composite Hurwitz polynomials of degree ≤ 3 in $h(\mathbb{Z}, \mathbb{Q})$ to be irreducible.

1. Introduction

Let R be a commutative ring with identity and $H(R)$ be the set of formal expressions of the form $\sum_{n=0}^{\infty} a_n x^n$, where $a_n \in R$. Addition on $H(R)$ is defined termwise. A multiplication, called $*$-product, on $H(R)$ is defined as follows: For $f = \sum_{n=0}^{\infty} a_n x^n, g = \sum_{n=0}^{\infty} b_n x^n \in H(R)$,

$$f * g = \sum_{n=0}^{\infty} c_n x^n, \ c_n = \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k},$$

where $\binom{n}{k} = \frac{n!}{(n-k)!k!}$ for nonnegative integers $n \geq k$. Keigher [4] showed that $H(R)$ is a commutative ring with identity under these two operations and then in [5] called $H(R)$ the *ring of Hurwitz series* over R. The *ring $h(R)$ of Hurwitz polynomials* over R is the subring of $H(R)$ consisting of formal expressions of the form $\sum_{k=0}^{n} a_k x^k$, *i.e.*, $h(R) = (R[x], +, *)$. After Keigher, many works on the rings of Hurwitz series and Hurwitz polynomials have been done ([1, 2, 6–9]).

For an extension $R \subseteq D$ of commutative rings with identity, let $H(R, D) = \{f \in H(D) \mid$ the constant term of f belongs to $R\}$ (resp., $h(R, D) = \{f \in h(D) \mid$ the constant term of f belongs to $R\}$). Then $H(R, D)$ (resp., $h(R, D)$) is a commutative ring with identity. We call $H(R, D)$ (resp., $h(R, D)$) a *ring of composite Hurwitz series* (resp., *a ring of composite Hurwitz polynomial*). More precisely, $H(R, D)$ (resp.,

Received March 31, 2022. Revised June 30, 2022. Accepted July 29, 2022.
2010 Mathematics Subject Classification: 13A05, 13A15, 13F15, 13F20.
Key words and phrases: Composite Hurwitz polynomial ring, irreducible composite Hurwitz polynomial, quasi-primary, atomic.
† This work was supported by Research Fund from Chosun University, 2019.
© The Kangwon-Kyungki Mathematical Society, 2022.
This is an Open Access article distributed under the terms of the Creative commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0/) which permits unrestricted non-commercial use, distribution and reproduction in any medium, provided the original work is properly cited.

$h(R, D)$) is a subring of $H(D)$ (resp., $h(D)$) containing $H(R)$ (resp., $h(R)$), *i.e.*, $H(R) \subseteq H(R, D) \subseteq H(D)$ (resp., $h(R) \subseteq h(R, D) \subseteq h(D)$).

Let R be a commutative ring with identity. An ideal Q of R is called *quasi-primary* if its radical $\sqrt{Q}$ is a prime ideal. Quasi-primary ideals in a commutative ring has been introduced by Fuchs [3]. We say that an element a of R is quasi-primary if the principal ideal (a) is quasi-primary.

Let $\mathbb{Z}$ be the ring of integers and $\mathbb{Q}$ be the field of rational numbers. Then $h(\mathbb{Z}) \subset h(\mathbb{Z}, \mathbb{Q}) \subset h(\mathbb{Q})$. It follows from [5, Proposition 2.4] that $h(\mathbb{Q}) \cong \mathbb{Q}[x]$, hence $h(\mathbb{Q})$ is a UFD. Note that $h(\mathbb{Z})$ is not a UFD by [9, Remark 2.5], hence $h(\mathbb{Z}) \ncong \mathbb{Z}[x]$. By [6, Theorem 2.4], $h(\mathbb{Z})$ satisfies the ascending chain condition on principal ideals (ACCP). Hence $h(\mathbb{Z})$ is atomic, that is, every nonzero nonunit element of $h(\mathbb{Z})$ is a finite $*$-product of irreducible elements.

In this paper, we investigate factorizations of the elements of $h(\mathbb{Z}, \mathbb{Q})$. In Section 2, we show that every nonzero nonunit element of $h(\mathbb{Z}, \mathbb{Q})$ is a finite $*$-product of quasi-primary elements and irreducible elements. In Section 3, we give a necessary and sufficient condition for composite Hurwitz polynomials $f \in h(\mathbb{Z}, \mathbb{Q})$ of degree ≤ 3 to be irreducible by using a relation between usual polynomials in $\mathbb{Q}[x]$ and composite Hurwitz polynomials in $h(\mathbb{Z}, \mathbb{Q})$. We also determine a condition for $f \in h(\mathbb{Z}, \mathbb{Q})$ of degree 4 to be factored into $f = g * h$, where g and h are elements of $h(\mathbb{Z}, \mathbb{Q})$ of degree 1 and 3, respectively.

2. Quasi-primary and irreducible composite Hurwitz polynomials

Let R be a commutative ring with identity. We recall that a nonzero nonunit element $u \in R$ is irreducible if $u = ab$ for some $a, b \in R$, then either a or b is a unit in R. We say that a nonzero nonunit element $a \in R$ is quasi-primary if the radical $\sqrt{(a)}$ of principal ideal (a) is a prime ideal of R. In this section, we classify quasi-primary elements and irreducible elements of $h(\mathbb{Z}, \mathbb{Q})$, and then show that every nonzero nonunit element of $h(\mathbb{Z}, \mathbb{Q})$ is a finite $*$-product of quasi-primary and irreducible elements of $h(\mathbb{Z}, \mathbb{Q})$. We start with known results on the ring $h(R, D)$, where $R \subseteq D$ is an extension of integral domains with characteristic zero.

Proposition 2.1. (cf. [6]) *Let $R \subseteq D$ be an extension of integral domains with characteristic zero. Then we have the following.*

1. *The ring $h(R, D)$ is an integral domain.*
2. *An element $f = \sum_{i=0}^{n} a_i x^i \in h(R, D)$ is a unit if and only if $f = a_0$ is unit in R.*
3. *$h(R, D)$ satisfies the ACCP if and only if $\bigcap_{n \geq 1} a_1 \cdots a_n D = (0)$ for each infinite sequence $(a_n)_{n \geq 1}$ consisting of nonzero nonunits of R.*

By Proposition 2.1 (3), note that $h(\mathbb{Z})$ and $h(\mathbb{Q})$ satisfy the ACCP. So $h(\mathbb{Z})$ and $h(\mathbb{Q})$ are atomic. However, $h(\mathbb{Z}, \mathbb{Q})$ does not satisfy the ACCP. Hence $h(\mathbb{Z}, \mathbb{Q})$ need not be atomic. For a commutative ring R with identity, let $U(R)$ be the set of units of R. Then it is clear that $U(h(\mathbb{Z}, \mathbb{Q})) = \{f \in h(\mathbb{Z}, \mathbb{Q}) \mid f = \pm 1\}$.

For a nonzero element $f = \sum_{i=0}^{n} a_n x^n \in h(\mathbb{Z}, \mathbb{Q})$, the *order* (resp., *degree*) of f, denoted by $\mathrm{ord}(f)$ (resp., $\deg(f)$), is the smallest (resp., largest) nonnegative integer m such that $a_m \neq 0$.

Lemma 2.2. *Let S be the set of element f of $h(\mathbb{Z}, \mathbb{Q})$ such that $f(0) \neq 0$. Then we have the following.*

1. *ord*$(f * g) =$ *ord*$(f) +$ *ord*(g)*, and deg*$(f * g) =$ *deg*$(f) +$ *deg*(g) *for* $f, g \in h(\mathbb{Z}, \mathbb{Q})$.
2. S *is a saturated multiplicative subset of* $h(\mathbb{Z}, \mathbb{Q})$.

Proof. (1) Since $\mathbb{Z}$ and $\mathbb{Q}$ are integral domains with characteristic zero, it is easily obtained by direct computations.

(2) Let $f, g, h \in h(\mathbb{Z}, \mathbb{Q})$ such that $f = g * h$. By (1), $\mathrm{ord}(f) = 0$ if and only if $\mathrm{ord}(g) = \mathrm{ord}(h) = 0$. Hence S is a saturated multiplicative set.

□

A subset S of a commutative ring R with identity is said to satisfy the ACCP if there does not exist a strictly infinite ascending chain of principal ideals of R generated by elements in S. Recall that for an $f \in h(\mathbb{Z}, \mathbb{Q})$, the principal ideal $(f) = \{f * h \mid h \in h(\mathbb{Z}, \mathbb{Q})\}$. For an $f \in h(\mathbb{Z}, \mathbb{Q})$ and $n \geq 1$, we denote the n-th Hurwitz power of f by $f^{(n)}$, that is, $f^{(n)} = f * \cdots * f (n \text{ times})$. Also, for an $f \in h(\mathbb{Z}, \mathbb{Q})$ and a nonnegative integer n, $f(n)$ stands for the coefficient of x^n in f.

Proposition 2.3. *Let S be the set of element f of $h(\mathbb{Z}, \mathbb{Q})$ such that $f(0) \neq 0$. Then we have the following.*

1. *A constant composite Hurwitz polynomial $f = a \in h(\mathbb{Z}, \mathbb{Q})$ is irreducible if and only if $a = \pm p$, where p is prime in $\mathbb{Z}$.*
2. *The set S satisfies the ACCP. Hence every nonunit element f in S is a $*$-product of irreducible elements of $h(\mathbb{Z}, \mathbb{Q})$.*
3. *For $0 \neq \alpha \in \mathbb{Q}$, αx is quasi-primary.*
4. *For every positive integer n and $0 \neq \alpha \in \mathbb{Q}$, αx^n is a $*$-product of quasi-primary elements of $h(\mathbb{Z}, \mathbb{Q})$.*

Proof. (1) Clear.

(2) Let $f \in S$. If $f = g * h$, then $g, h \in S$, and $\deg(g) \leq \deg(f)$ by Lemma 2.2. Moreover, if $f = g * h$ and $\deg(f) = \deg(g)$, then $f = a * g = ag$ for some $0 \neq a \in \mathbb{Z}$. Suppose that $(f_1) \subseteq (f_2) \subseteq \cdots$ is an infinite ascending chain of principal ideals of $h(\mathbb{Z}, \mathbb{Q})$, where each $f_i \in S$. Since $\deg(f_i) \geq \deg(f_{i+1})$ for each i, there exists $m \geq 1$ such that $\deg(f_i) = \deg(f_m)$ for all $i \geq m$. By considering such subsequence, we may assume that $\deg(f_i) = n$ for all $i \geq 1$. Since $(f_i) \subseteq (f_{i+1})$ and $\deg(f_i) = \deg(f_{i+1})$ for each i, $f_i = a_i f_{i+1}$ for $0 \neq a_i \in \mathbb{Z}$. Hence $f_i(0) = a_i f_{i+1}(0)$ for each $i \geq 1$. Since $f_i(0) \in \mathbb{Z}$, $(f_1(0)) \subseteq (f_2(0)) \subseteq \cdots$ is an ascending chain of principal ideals of $\mathbb{Z}$. Therefore there exists $i_0 \geq 1$ such that a_i is unit in $\mathbb{Z}$ for all $i \geq i_0$. Thus $(f_i) = (f_{i_0})$ for all $i \geq i_0$.

(3) Note that for an element $\alpha x \in h(\mathbb{Z}, \mathbb{Q})$, where $0 \neq \alpha \in \mathbb{Q}$, we have

$$\begin{aligned}(\alpha x) &= \{\alpha x * h \mid h = \sum_{i=0}^{n} a_i x^i \in h(\mathbb{Z}, \mathbb{Q})\} \\ &= \{a_0 \alpha x + 2a_1 \alpha x^2 + \cdots + (n+1) a_n \alpha x^{n+1} \mid a_0 \in \mathbb{Z}, a_i \in \mathbb{Q} \text{ for } i \geq 1\}.\end{aligned}$$

Hence if $f \in h(\mathbb{Z}, \mathbb{Q})$ with $\mathrm{ord}(f) \geq 2$, then

$$\begin{aligned}f &= a_2 x^2 + a_3 x^3 + \cdots + a_n x^n \\ &= \alpha x * (\frac{a_2}{2\alpha} x + \frac{a_3}{3\alpha} x^2 + \cdots + \frac{a_n}{n\alpha} x^{n-1}) \in (\alpha x),\end{aligned}$$

where $a_i \in \mathbb{Q}$ for $i = 2, \ldots, n$.

We claim that for an element $f \in h(\mathbb{Z}, \mathbb{Q})$ and $0 \neq \alpha \in \mathbb{Q}$, $f \in \sqrt{(\alpha x)}$ if and only if $f(0) = 0$. If $f \in \sqrt{(\alpha x)}$, then $f^{(n)} \in (\alpha x)$ for some $n \geq 1$. Thus $f^{(n)} = \alpha x * g$

for some $g \in h(\mathbb{Z}, \mathbb{Q})$. By Lemma 2.2, $\mathrm{ord}(f^{(n)}) \geq 1$. Hence $f^{(n)}(0) = f(0)^n = 0$. Since $f(0) \in \mathbb{Z}$, $f(0) = 0$. If $f \in h(\mathbb{Z}, \mathbb{Q})$ such that $f(0) = 0$, then $f^{(2)} = f * f$ is an element of order ≥ 2 by Lemma 2.2. Thus $f^{(2)} \in (\alpha x)$, hence $f \in \sqrt{(\alpha x)}$. Now we show that $\sqrt{(\alpha x)}$ is prime. Let $f * g \in \sqrt{(\alpha x)}$ for $f, g \in h(\mathbb{Z}, \mathbb{Q})$. By the claim above, $(f * g)(0) = f(0)g(0) = 0$. Thus, either $f(0) = 0$ or $g(0) = 0$. Hence, either $f \in \sqrt{(\alpha x)}$ or $g \in \sqrt{(\alpha x)}$. Therefore αx is quasi-primary.

(4) We prove it by induction on n. If $n = 1$, then it is clear by (3). Assume that αx^n is a $*$-product of quasi-primary elements. Since $\alpha x^{n+1} = \alpha x^n * \frac{1}{n+1} x$, αx^{n+1} is a $*$-product of quasi-primary elements in $h(\mathbb{Z}, \mathbb{Q})$. □

Remark 2.4. *For a nonzero integer k, consider $\frac{1}{k}x \in h(\mathbb{Z}, \mathbb{Q})$. Since $\frac{1}{k}x = 2 * \frac{1}{2k}x$ and $U(h(\mathbb{Z}, \mathbb{Q})) = U(\mathbb{Z}) = \{\pm 1\}$, we have $(\frac{1}{k}x) \subset (\frac{1}{2k}x)$. Hence $(\frac{1}{k}x) \subset (\frac{1}{2k}x) \subset \frac{1}{2^2k}x) \subset \cdots$ is a strictly infinite ascending chain of principal ideals of $h(\mathbb{Z}, \mathbb{Q})$. Note that if $f \mid \frac{1}{k}x$ for $f \in h(\mathbb{Z}, \mathbb{Q})$, then either f is constant or f is an element of $ord(f) = deg(f) = 1$. Therefore, $\frac{1}{k}x$ cannot be written as a (finite) $*$-product of irreducible elements of $h(\mathbb{Z}, \mathbb{Q})$.*

Theorem 2.5. *Every nonzero nonunit element of $h(\mathbb{Z}, \mathbb{Q})$ can be written as a finite $*$-product of quasi-primary elements and irreducible elements of $h(\mathbb{Z}, \mathbb{Q})$.*

Proof. Let f be a nonzero nonunit element of $h(\mathbb{Z}, \mathbb{Q})$. If $f(0) \neq 0$, then f is a $*$-product of irreducible elements by Proposition 2.3. So we may assume that $\mathrm{ord}(f) = m \geq 1$. Thus, $f = \alpha_m x^m + \alpha_{m+1} x^{m+1} + \cdots + \alpha_n x^n$, where $\alpha_i \in \mathbb{Q}$ for each $m \leq i \leq n$. Since $0 \neq f(m) = \alpha_m \in \mathbb{Q}$, we can write f as follows:

$$\begin{aligned} f &= \alpha_m x^m + \alpha_{m+1} x^{m+1} + \cdots + \alpha_n x^n \\ &= (\alpha_m x^m) * (1 + \frac{\alpha_{m+1}}{\alpha_m \binom{m+1}{1}} x + \frac{\alpha_{m+2}}{\alpha_m \binom{m+2}{2}} x^2 + \cdots + \frac{\alpha_n}{\alpha_m \binom{n}{m}} x^{n-m}). \end{aligned}$$

By Proposition 2.3, f is a $*$-product of quasi-primary elements and irreducible elements in $h(\mathbb{Z}, \mathbb{Q})$. □

3. Irreducible composite Hurwitz polynomials of degree ≤ 3

In this section, we give a necessary and sufficient condition for composite Hurwitz polynomials $f \in h(\mathbb{Z}, \mathbb{Q})$ of degree ≤ 3 to be irreducible by using a relation between usual polynomials in $\mathbb{Q}[x]$ and composite Hurwitz polynomials in $h(\mathbb{Z}, \mathbb{Q})$. We also determine a condition for $f \in h(\mathbb{Z}, \mathbb{Q})$ of degree 4 to be factored into $f = g * h$, where g and h are elements of $h(\mathbb{Z}, \mathbb{Q})$ of degree 1 and 3, respectively.

Since $U(h(\mathbb{Z}, \mathbb{Q})) = \{\pm 1\}$, a nonzero constant element f of $h(\mathbb{Z}, \mathbb{Q})$ is irreducible if and only if $f = \pm p$ is prime in $\mathbb{Z}$. To determine whether $f \in h(\mathbb{Z}, \mathbb{Q})$ is irreducible or not, we consider the case when f is an element of $h(\mathbb{Z}, \mathbb{Q})$ of degree ≥ 1. We start this section with the following simple observation. Recall that for an $f \in h(\mathbb{Z}, \mathbb{Q})$ and a nonnegative integer n, $f(n)$ stands for the coefficient of x^n in f, hence $f(0)$ stands for the constant term of f.

Lemma 3.1. *Let f be a composite Hurwitz polynomial of degree ≥ 1 in $h(\mathbb{Z}, \mathbb{Q})$. If either $f(0) = 0$ or $f(0) \neq \pm 1$, then f is reducible.*

Proof. Let $f = \sum_{i=0}^{n} a_i x^i \in h(\mathbb{Z}, \mathbb{Q})$. If $a_0 = 0$, then $f = m * (\frac{a_n}{m} x^n + \cdots + \frac{a_1}{m} x)$ for any nonzero integer m. If $a_0 \neq \pm 1$, then $f = a_0 * (\frac{a_n}{a_0} x^n + \cdots + \frac{a_1}{a_0} x + 1)$. Since $U(h(\mathbb{Z}, \mathbb{Q})) = \{\pm 1\}$, f is reducible. □

From Lemma 3.1, to determine whether an element $f \in h(\mathbb{Z}, \mathbb{Q})$ is irreducible, we only consider the case when $f(0) = 1$. For $0 \neq a \in \mathbb{Q}$, it is clear that $f = ax + 1 \in h(\mathbb{Z}, \mathbb{Q})$ is irreducible, hence consider the case when f is an element of $h(\mathbb{Z}, \mathbb{Q})$ of degree ≥ 2.

THEOREM 3.2. *Let f be an element of $h(\mathbb{Z}, \mathbb{Q})$ of degree 2. Then the followings are equivalent.*

1. $f = a_2 x^2 + a_1 x + 1$ *is irreducible in* $h(\mathbb{Z}, \mathbb{Q})$.
2. $\widetilde{f} = x^2 - a_1 x + \frac{1}{2} a_2$ *is irreducible in* $\mathbb{Q}[x]$.

Proof. (1) $\Leftrightarrow$ (2) Note that for $\alpha, \beta \in \mathbb{Q}$,

$$(\alpha x + 1) * (\beta x + 1) = 2\alpha\beta x^2 + (\alpha + \beta)x + 1.$$

Hence $f = a_2 x^2 + a_1 x + 1 = (\alpha x + 1) * (\beta x + 1)$ in $h(\mathbb{Z}, \mathbb{Q})$ if and only if $\alpha + \beta = a_1, \alpha\beta = \frac{1}{2} a_2$ if and only if $\widetilde{f} = x^2 - a_1 x + \frac{1}{2} a_2 = (x - \alpha)(x - \beta)$ in $\mathbb{Q}[x]$. Therefore f is irreducible in $h(\mathbb{Z}, \mathbb{Q})$ if and only if $\widetilde{f}$ is irreducible in $\mathbb{Q}[x]$. □

THEOREM 3.3. *Let f be an element of $h(\mathbb{Z}, \mathbb{Q})$ of degree 3. Then the followings are equivalent.*

1. $f = a_3 x^3 + a_2 x^2 + a_1 x + 1$ *is irreducible in* $h(\mathbb{Z}, \mathbb{Q})$.
2. $\widetilde{f} = 6x^3 - 6a_1 x^2 + 3a_2 x - a_3$ *is irreducible in* $\mathbb{Q}[x]$.

Proof. (2) $\Rightarrow$ (1) Suppose that f is reducible in $h(\mathbb{Z}, \mathbb{Q})$. There exist $b_1, b_2, c_1 \in \mathbb{Q}$ such that

$$\begin{aligned} f &= (b_2 x^2 + b_1 x + 1) * (c_1 x + 1) \\ &= 3b_2 c_1 x^3 + (2b_1 c_1 + b_2)x^2 + (b_1 + c_1)x + 1 \\ &= a_3 x^3 + a_2 x^2 + a_1 x + 1. \end{aligned}$$

Hence $a_3 = 3b_2 c_1, a_2 = 2b_1 c_1 + b_2$, and $a_1 = b_1 + c_1$. So we have

$$\begin{cases} b_1 = a_1 - c_1, \\ b_2 = a_2 - 2b_1 c_1 = a_2 - 2a_1 c_1 + 2c_1^2, \\ a_3 = 3b_2 c_1 = 3a_2 c_1 - 6a_1 c_1^2 + 6c_1^3. \end{cases}$$

Therefore, $\widetilde{f} = 6x^3 - 6a_1 x^2 + 3a_2 x - a_3 \in \mathbb{Q}[x]$ has a rational root c_1. Thus $\widetilde{f}$ is reducible in $\mathbb{Q}[x]$.

(1) $\Rightarrow$ (2) Suppose that $\widetilde{f}$ is reducible in $\mathbb{Q}[x]$. Let $c_1 \in \mathbb{Q}$ be a root of $\widetilde{f}$. Then there exist rational numbers b_0 and b_1 such that

$$\begin{aligned} \widetilde{f} &= 6x^3 - 6a_1 x^2 + 3a_2 x - a_3 \\ &= (x - c_1)(6x^2 + b_1 x + b_0). \end{aligned}$$

Hence $-6a_1 = b_1 - 6c_1, 3a_2 = b_0 - b_1c_1$, and $a_3 = b_0c_1$. So we have

$$\begin{aligned} f &= a_3x^3 + a_2x^2 + a_1x + 1 \\ &= b_0c_1x^3 + \frac{b_0 - b_1c_1}{3}x^2 + \frac{-b_1 + 6c_1}{6}x + 1 \\ &= (\frac{b_0}{3}x^2 - \frac{b_1}{6}x + 1) * (c_1x + 1). \end{aligned}$$

Hence f is reducible in $h(\mathbb{Z}, \mathbb{Q})$.

□

For $0 \neq a \in \mathbb{Q}$, $x^3 - a \in \mathbb{Q}[x]$ has only one real root $\sqrt[3]{a}$. So we have the following.

COROLLARY 3.4. *Let $f = ax^3 + 1$ be an element of $h(\mathbb{Z}, \mathbb{Q})$ of degree 3. Then the followings are equivalent.*

1. *$f = ax^3 + 1$ is reducible in $h(\mathbb{Z}, \mathbb{Q})$.*
2. *$\widetilde{f} = 6x^3 - a$ is reducible in $\mathbb{Q}[x]$.*
3. *$a = 6b^3$ for some $0 \neq b \in \mathbb{Q}$.*

Now we give a necessary and sufficient condition for an element f in $h(\mathbb{Z}, \mathbb{Q})$ of degree 4 to be factored into $f = g * h$, where g and h are elements in $h(\mathbb{Z}, \mathbb{Q})$ of $\deg(g) = 3$ and $\deg(h) = 1$.

PROPOSITION 3.5. *Let $f = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + 1$ be an element of $h(\mathbb{Z}, \mathbb{Q})$ of $\deg(f) = 4$. Then the following are equivalent.*

1. *$f = g*h$, where g and h are elements of $h(\mathbb{Z}, \mathbb{Q})$ with degree 3 and 1, respectively.*
2. *$\widetilde{f} = 24x^4 - 24a_1x^3 + 12a_2x^2 - 4a_3x + a_4 \in \mathbb{Q}[x]$ has a rational root.*

Proof. (1) ⇒ (2) Suppose that $f = g * h$, where $g, h \in h(\mathbb{Z}, \mathbb{Q})$ of $\deg(g) = 3$ and $\deg(h) = 1$. Since $f(0) = 1$, there exist rational numbers b_1, b_2, b_3 and c_1 such that

$$\begin{aligned} f &= (b_3x^3 + b_2x^2 + b_1x + 1) * (c_1x + 1) \\ &= 4b_3c_1x^4 + (b_3 + 3b_2c_1)x^3 + (b_2 + 2b_1c_1)x^2 + (b_1 + c_1)x + 1 \\ &= a_4x^4 + a_3x^3 + a_2x^2 + a_1x + 1. \end{aligned}$$

Hence $a_4 = 4b_3c_1, a_3 = b_3 + 3b_2c_1, a_2 = b_2 + 2b_1c_1$, and $a_1 = b_1 + c_1$. So we have

$$\begin{cases} b_1 = a_1 - c_1, \\ b_2 = a_2 - 2b_1c_1 = a_2 - 2a_1c_1 + 2c_1^2, \\ b_3 = a_3 - 3b_2c_1 = a_3 - 3a_2c_1 + 6a_1c_1^2 - 6c_1^3, \\ a_4 = 4b_3c_1 = -24c_1^4 + 24a_1c_1^3 - 12a_2c_1^2 + 4a_3c_1. \end{cases}$$

Therefore, c_1 is a rational root of $\widetilde{f} = 24x^4 - 24a_1x^3 + 12a_2x^2 - 4a_3x + a_4 \in \mathbb{Q}[x]$.

(2) ⇒ (1) Suppose that $\widetilde{f} \in \mathbb{Q}[x]$ has a rational root c_1. Then there exist rational numbers b_0, b_1, b_2, and b_3 such that

$$\begin{aligned} \widetilde{f} &= (x - c_1)(24x^3 + b_2x^2 + b_1x + b_0) \\ &= 24x^4 - 24a_1x^3 + 12a_2x^2 - 4a_3x + a_4. \end{aligned}$$

Hence $-24a_1 = b_2 - 24c_1, 12a_2 = b_1 - b_2c_1, -4a_3 = b_0 - b_1c_1$, and $a_4 = -b_0c_1$. So we have

$$\begin{aligned} f &= a_4x^4 + a_3x^3 + a_2x^2 + a_1x + 1 \\ &= -b_0c_1x^4 + \frac{b_1c_1 - b_0}{4}x^3 + \frac{b_1 - b_2c_1}{12}x^2 + \frac{-b_2 + 24c_1}{24}x + 1 \\ &= (-\frac{b_0}{4}x^3 + \frac{b_1}{12}x^2 - \frac{b_2}{24}x + 1) * (c_1x + 1). \end{aligned}$$

□

Acknowledgments

We would like to thank the referees for several valuable suggestions. This paper (Section 3) contains part of a master's thesis of I.M.Oh done at Chosun University.

References

[1] A. Benhissi, *Ideal structure of Hurwitz series ring*, Contrib. Alg. Geom. **48** (1997) 251–256.
[2] A. Benhissi and F. Koja, *Basic properties of Hurwitz series rings*, Ric. Mat. **61** (2012) 255–273.
[3] L. Fuchs, *On quasi-primary ideals*, Acta. Sci. Math. (Szeged), **11** (1947) 174–183.
[4] W.F. Keigher, *Adjunctions and comonads in differential algebra*, Pacific J. Math. **59** (1975) 99–112.
[5] W.F. Keigher, *On the ring of Hurwitz series*, Comm. Algebra **25** (1997) 1845–1859.
[6] J.W. Lim and D.Y. Oh, *Composite Hurwitz rings satisfying the ascending chain condition on principal ideals*, Kyungpook Math. J. **56** (2016) 1115–1123.
[7] J.W. Lim and D.Y. Oh, *Chain conditions on composite Hurwitz series rings*, Open Math. **15** (2017) 1161–1170.
[8] Z. Liu, *Hermite and PS-rings of Hurwitz series*, Comm. Algebra **28** (2000) 299–305.
[9] D.Y. Oh and Y.L. Seo, *Irreducibility of Hurwitz polynomials over the ring of integers*, Korean J. Math. **27** (2019) 465–474.

Dong Yeol Oh
Department of Mathematics Education, Chosun University,
Gwangju 61452, Republic of Korea
E-mail: dyoh@chosun.ac.kr, dongyeol70@gmail.com

Ill Mok Oh
Department of Mathematics Education, Chosun University,
Gwangju 61452, Republic of Korea
E-mail: skdlfahr@naver.com