JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **22**, No. 3, September 2009

COMPOSITION OF POLYNOMIALS OVER A FIELD

EunMi Choi*

Abstract. This work studies about the composition polynomial $f(g(x))$ that preserves certain properties of $f(x)$ and $g(x)$. We shall investigate necessary and sufficient conditions of $f(x)$ and $g(x)$ to be $f(g(x))$ is separable, solvable by radical or split completely. And we find relationship of Galois groups of $f(g(x))$, $f(x)$ and of $g(x)$.

1. Introduction

Let K be a field and let $f(x)$ and $g(x)$ be polynomials in $K[x]$. We denote the composite of $f(x)$ and $g(x)$ by $f(g(x))$, and define the iterates of $f(x)$ by $f_1(x) = f(x)$, $f_2(x) = f(f_1(x))$ (the 2nd iterate) and $f_{r+1}(x) = f(f_r(x))$ (the rth iterate) for all $r \geq 1$.

During last some decades many researcher have asked an interesting question that what properties of $f(x)$ are preserved in the composition $f_r(x)$ of $f(x)$. There are some examples in [2], [5] and [6]. For instance, $f(x) = x^2 + 10x + 17 \in \mathbb{Z}[x]$ is irreducible but the 2nd iterate $f_2(x) = (x^2 + 12x + 34)(x^2 + 8x + 14)$ is reducible. For the separability, $g(x) = x^2 - 1$ is separable and split completely in $\mathbb{Q}[x]$, but $g_2(x) = x^2(x^2 - 2)$ is inseparable and does not split completely in $\mathbb{Q}$. Moreover for the solvability, $h(x) = x^5 - 5x + 12$ is solvable by radical over $\mathbb{Q}$ but $h_2(x)$ is not solvable by radical. However there are also examples such as $f(x) = x^2 - x + 1 \in \mathbb{Z}[x]$, that not only $f(x)$ but all nth iterates $f_n(x)$ are irreducible ([5]).

Furthermore it was proved in [2] that there exist a polynomial $f(x) \in K[x]$ such that the first r iterations of $f(x)$ posses certain property, such as irreducibility, separability, splitting completely, and solvability by radicals, but the next iterate does not hold. From that point, another natural question was raised that over which fields K can such examples

Received June 03, 2009; Accepted August 14, 2009.
2000 Mathematics Subject Classification: Primary 11D09, 12F10, 20B05.
Key words and phrases: iterated polynomial, Galois group, Wreath product.
*Supported by Hannam University Research Fund 2009.

exist? In [2], K was assumed as a Hilbertian field, and it was proved that there always exist irreducible polynomials $f(x)$ and $g(x) \in K[x]$ such that both $f(x)$ and $g(x)$ are solvable by radical over K and $f(g(x))$ is irreducible in $K[x]$ however $f(g(x))$ is not solvable by radical over K.

In this paper, we study composition polynomials $f(g(x))$ that preserve certain properties of $f(x)$ and $g(x)$. We shall investigate necessary and sufficient conditions of $f(x)$ and $g(x)$ to be $f(g(x))$ is separable, solvable by radical or splits completely. And we find relationships between Galois groups of $f(g(x))$, $f(x)$ and of $g(x)$.

2. Separability and solvability of composition

A well known property about the composition $f(g(x))$ of $f(x)$ and $g(x)$ due to Capelli is as follows.

LEMMA 2.1. [6] *Let $f(x)$ and $g(x)$ be in $K[x]$.*

(1) *Let β be a root of $f(x)$. Then every root of $g(x) - \beta$ is a root of $f(g(x))$. And if α is a root of $f(g(x))$ then $g(\alpha)$ is a root of $f(x)$.*
(2) *The splitting field of $f(x)$ over K is contained in the splitting field of $f(g(x))$ over K.*

In fact, if β is a root of $f(x)$ and θ is a root of $g(x)-\beta$ then $f(g(\theta)) = f(\beta) = 0$. If $\alpha_1, \alpha_2, \cdots, \alpha_l$ $(l > 0)$ are roots of $f(g(x))$ in some splitting field over K then $g(\alpha_i)$ gives all the zeros of $f(x)$ thus the splitting field of f is contained in the splitting field of $f(g(x))$.

LEMMA 2.2. [2] *(Capelli's Lemma) Let $f(x), g(x) \in K[x]$. $f(g(x))$ is irreducible in $K[x]$ if and only if $f(x)$ is irreducible in $K[x]$ and $g(x)-\beta$ is irreducible in $K(\beta)[x]$ for every root β of $f(x)$.*

In fact, if θ is a root of $g(x) - \beta$ where β is a root of $f(x)$, then θ is a root of $f(g(x))$, and the dimensions $[K(\beta) : K]$ and $[K(\theta) : K(\beta)]$ are less than or equal to $\deg f(x)$ and $\deg(g(x) - \beta) = \deg g(x)$ respectively. Thus,

$f(g(x))$ is irreducible in $K[x]$ if and only if $[K(\theta) : K] = \deg f(g(x))$
if and only if $[K(\theta) : K(\beta)][K(\beta) : K] = \deg f(x) \cdot \deg g(x)$
if and only if $[K(\beta) : K] = \deg f(x)$ and $[K(\theta) : K(\beta)] = \deg g(x)$
if and only if $f(x)$ is irreducible in $K[x]$ and $g(x) - \beta$ is irreducible in $K(\beta)[x]$.

We now discuss about situations that $f(g(x))$ is separable over K, and then we ask whether the separability can be replaced by split completely or solvability by radical. Throughout this paper, we denote $S_{f \circ g}$ and

S_f the splitting fields for $f(g(x))$ and $f(x)$ over K respectively, and let $S_{g-\beta}$ be the splitting field for $g(x)-\beta$ over $K(\beta)$ where β is a root of $f(x)$.

THEOREM 2.3. *Let K be a field and let $f(x)$ and $g(x)$ be in $K[x]$.*

(1) *$f(g(x))$ is separable over K if and only if both $f(x)$ is separable over K and $g(x)-\beta$ is separable over $K(\beta)$ for every root β of $f(x)$.*
(2) *The term 'separability' in (1) can be replaced by 'splitting completely'.*
(3) *The term 'separability' in (1) can be replaced by 'solvability of radical'.*

Proof. Let $\deg f = n$ and $\deg g = m$. Let $\bar{K}$ be the algebraic closure of K. If $f(g(x))$ is separable over K then $f(g(x))$ has nm distinct roots in $\bar{K}$. Let $\beta = \beta_1, \beta_2, ..., \beta_n$ be roots of $f(x)$ in $\bar{K}$. Since $\deg(g(x)-\beta_i) = m$ for all $1 \le i \le n$, $g(x)-\beta_i$ has at most m distinct roots in $\bar{K}$. And since roots of $g(x)-\beta_i$ are roots of $f(g(x))$ due to Lemma 2.1, we may write $f(g(x)) = \prod_{i=1}^{n}(g(x)-\beta_i)$. Because $f(g(x))$ has exactly nm distinct roots in $\bar{K}$, there must exist n distinct β_i's and m distinct roots of each $g(x)-\beta_i$, this means that both $f(x)$ and $g(x)-\beta_i$ are separable polynomials.

Conversely, if $f(x)$ has n distinct roots $\beta = \beta_1, \beta_2, ..., \beta_n$, and $g(x)-\beta_i$ $(1 \le i \le n)$ has m distinct roots in $\bar{K}$ then $f(g(x)) = \prod_{i=1}^{n}(g(x)-\beta_i)$ has nm distinct roots in $\bar{K}$ thus $f(g(x))$ is separable over K.

(2) If $f(g(x))$ splits completely in a field F over K then $S_{f\circ g}$ is contained in F. Since S_f and $S_{g-\beta}$ are contained in $S_{f\circ g} \subseteq F$ due to Lemma 2.1, both $f(x)$ and $g(x)-\beta$ split completely in F.

Conversely, suppose that both $f(x) \in K[x]$ and $g(x)-\beta \in K(\beta)[x]$ split completely in F. Let α be a root of $f(g(x))$. Since $g(\alpha)$ is a root of $f(x)$, $g(\alpha)$ belongs to F. By regarding β as $g(\alpha)$, α is a root of $g(x)-\beta \in K(\beta)[x] = K[x]$, thus α belongs to F.

(3) Now for the solvability, assume $f(g(x))$ is solvable by radical over K. Then the Galois group $\mathrm{Gal}\Big(f(g(x))/K\Big) = \mathrm{Gal}\Big(S_{f\circ g}/K\Big)$ is a solvable group. Since both S_f and $S_{g-\beta}$ are contained in $S_{f\circ g}$, $\mathrm{Gal}(f(x)/K) = \mathrm{Gal}\Big(S_f/K\Big)$ and

$$\mathrm{Gal}\Big(g(x)-\beta/K(\beta)\Big) = \mathrm{Gal}\Big(S_{g-\beta}/K(\beta)\Big)$$

are homomorphic images of $\mathrm{Gal}\Big(S_{f\circ g}/K\Big)$. Since the homomorphic image of solvable group is solvable, $f(x)$ is solvable by radical over K and $g(x)-\beta$ is solvable by radical over $K(\beta)$.

On the other hand, we assume $f(x)$ and $g(x)-\beta$ (β : any root of $f(x)$) are solvable by radical over K and $K(\beta)$ respectively. Let α be a root of $f(g(x))$. Then $g(\alpha)$ is a root of $f(x)\in K[x]$ since $f(g(\alpha))=0$. If we denote $g(\alpha)$ by β then α is a root of $g(x)-\beta\in K(\beta)[x]$, for $g(\alpha)-\beta=g(\alpha)-g(\alpha)=0$. Since $f(x)$ is solvable by radical, we have a tower of radical extension fields of K that

$$K<K(a_1)<\cdots<K(a_1,\ldots,a_s)<K(a_1,\ldots,a_s,\beta),$$

where $a_i\in\bar{K}$, $a_i^{v_i}\in K(a_1,\ldots,a_{i-1})$ for $v_i>0$ $(1\le i\le s)$, and $\beta^t\in K(a_1,\ldots,a_s)$ for $t>0$. And $g(x)-\beta$ are solvable by radical yields a tower of radical extension fields of $K(\beta)$ that,

$$K(\beta)<K(\beta,b_1)<\cdots<K(\beta,b_1,\ldots,b_u)<K(\beta,b_1,\ldots,b_u,\alpha),$$

where $b_j\in\bar{K}$, $b_j^{w_j}\in K(\beta,b_1,\ldots,b_{j-1})$ for $1\le j\le u$, and $\alpha^v\in K(\beta,b_1,\ldots,b_u)$ for some $v,w_j>0$. Combining the above two towers of fields, we get

$$\begin{aligned} K &< \ldots<K(a_1,\ldots,a_s,\beta)<K(\beta,b_1,a_1,\ldots,a_s)<\ldots \\ &< K(\beta,b_1,\ldots,b_u,\alpha,a_1,\ldots,a_s). \end{aligned}$$

This is clearly a radical extension tower over K containing the splitting field of $f(g(x))$, so $f(g(x))$ is solvable by radical. □

We have seen that there are irreducible polynomials $f(x)$ whose all iterations are irreducible, while there are also irreducible polynomials $g(x)$ whose iterations are not irreducible, for example $f(x)=x^2-x+1\in\mathbb{Z}[x]$ and $g(x)=x^2+10x+17\in\mathbb{Z}[x]$. We shall consider a family of irreducible polynomials whose all iterations are irreducible.

An irreducible polynomial $f(x)=\sum_{i=0}^{k}a_ix^i\in\mathbb{Z}[x]$ is called *p-Eisenstein* if the prime p satisfies the Eisenstein's criterion, that is, $p|a_0$, $p|a_1$, $\cdots$, $p|a_{k-1}$, $p\nmid a_k$, and $p^2\nmid a_0$.

Consider a polynomial $f(x)=x^3+2x^2+2x+2\in\mathbb{Q}[x]$. It is obvious that $f(x)$ is an irreducible polynomial by Eisenstein criterion with $p=2$. Moreover it can be checked by Maple package that $f_2(x)$ of degree 9 and $f_3(x)$ of degree 27 are irreducible.

THEOREM 2.4. *Every composition of irreducible polynomial of the form p-Eisenstein is irreducible.*

Proof. We shall show that, if f_1, f_2, $\cdots$, f_n are p-Eisenstein then $f_1 \circ f_2 \circ \cdots \circ f_n$ is p-Eisenstein. Let $f_1(x) = \sum_{i=0}^{k} a_i x^i$ and $f_2(x) = \sum_{i=0}^{s} b_i x^i$. The prime satisfies $p|a_0$, $p|a_1$, $\cdots$, $p|a_{k-1}$, $p \not| a_k$, and $p^2 \not| a_0$, and $p|b_0$, $p|b_1$, $\cdots$, $p|b_{s-1}$, $p \not| b_s$, and $p^2 \not| b_0$. By mod p, $f_1(x) \equiv a_k x^k$ and $f_2(x) \equiv b_s x^s$, thus

$$f_1(f_2(x)) \equiv f_1(b_s x^s) \equiv a_k (b_s x^s)^k = (a_k {b_s}^k) x^{sk} \pmod{p}.$$

This means that every coefficient of $f_1(f_2(x))$ except the largest degree term are all 0 by mod p, that is, divisible by p. If $p|a_k {b_s}^k$ then either $p|a_k$ or $p|b_s$, which is not true. Hence $p \not| a_k {b_s}^k$. Suppose p^2 divides the constant term of $f_1(f_2(x))$. The constant term of $f_1(f_2(x))$ is $(f_1 \circ f_2)(0) = f_1(f_2(0)) = f_1(b_0) = a_0 + a_1 b_0 + a_2 {b_0}^2 + \cdots + a_k {b_0}^k$. Since a_i $(1 \leq i < k)$ and b_0 are multiple of p, $a_i {b_0}^j$ are multiple of p^2 for all $1 \leq i < k$; $0 \leq j \leq k$. Hence if $p^2|(f_1 \circ f_2)(0)$ then it should be $p^2|a_0$, which is a contradiction. Thus $p^2 \not| f_1(f_2(0))$. Therefore $f_1(f_2(x))$ is p-Eisenstein.

Suppose that $f_1 \circ f_2 \circ \cdots \circ f_{n-1}$ is p-Eisenstein. Then $f_1 \circ f_2 \circ \cdots \circ f_n$ which is the composition $(f_1 \circ f_2 \circ \cdots \circ f_{n-1}) \circ f_n$ of two p-Eisenstein polynomials is p-Eisenstein. □

In next theorem, by taking $g(x)$ more specifically, for instance, as a binomial polynomial $g(x) = x^m - b$ $(m > 0)$, which is of course solvable by radical, we can prove that the composition of f and g is solvable by radical.

THEOREM 2.5. *Let $f(x)$ and $g(x) \in K[x]$. If f is solvable by radical and $g(x) = x^m - b$ $(b \in K)$ then $f(g(x))$ is solvable by radical.*

Proof. Let α be a root of $f(g(x))$. Since f is solvable by radical, $g(\alpha)$ which is a root of $f(x)$ has a radical expression, say $g(\alpha) = \sqrt[n]{u}$ for some $u \in K$. Thus $\sqrt[n]{u} = g(\alpha) = \alpha^m - b$ implies that $\alpha = \sqrt[m]{\sqrt[n]{u} + b}$, which is a radical expression over K. Hence $f(g(x))$ is solvable by radical. □

Remark that we do not know whether $g(f(x))$ is solvable in the above theorem.

3. Galois group of composite polynomials

The solvability by radical of polynomial has a strong relationship to the solvability of Galois group of the polynomial, so in this section we will concern the Galois group of composite polynomials.

THEOREM 3.1. *Let σ be any element in $Gal\Big(S_{f\circ g}/K\Big)$. And let β be a root of $f(x)$. Then*

(1) *$\sigma|_{S_f}$ belongs to $Gal\,(f(x)/K)$.*
(2) *If the restriction of σ to $K(\beta)$ is identity, then $\sigma|_{S_{g-\beta}}$ is contained in $Gal\,((g(x)-\beta)/K(\beta))$.*

Proof. We first note that $\mathrm{Gal}\Big(S_{f\circ g}/K\Big) = \mathrm{Gal}\Big(f(g(x))/K\Big)$. Let $n = \deg(f(x))$ and $m = \deg(g(x))$. We shall show that the restriction of σ to S_f maps roots of $f(x)$ to roots of $f(x)$.

We denote the roots of $f(g(x))$ over K by α_{ij} $(i = 1, \cdots, n;\ j = 1, \cdots, m)$. Let $\beta_1 = \beta, \cdots, \beta_n$ be zeros of $f(x)$ over K. Since $g(\alpha_{ij})$ are zeros of $f(x)$, we may correspond $g(\alpha_{ij}) = \beta_i$.

For any $\sigma \in \mathrm{Gal}\Big(S_{f\circ g}/K\Big)$, $\sigma(\alpha_{ij}) = \alpha_{i'j'}$ for some $1 \le i' \le n$; $1 \le j' \le m$, thus

$$\beta_{i'} = g(\alpha_{i'j'}) = g(\sigma(\alpha_{ij})) = \sigma(g(\alpha_{ij})) = \sigma(\beta_i).$$

Hence σ maps β_i to $\beta_{i'}$, so the restriction $\sigma|_{S_f}$ of σ to S_f belongs to $\mathrm{Gal}\Big(S_f/K\Big)$.

For (2), we will show that any automorphism over $S_{f\circ g}$ maps roots of $g(x)-\beta$ to roots of $g(x)-\beta$. Let $\theta_{i1}, \cdots, \theta_{im}$ be roots of $g(x)-\beta_i$ over $K(\beta_i)$. Then $g(\theta_{ij}) = \beta_i$ for $j = 1, \cdots, m$, and every θ_{ij} $(i = 1, \cdots, n)$ are roots of $f(g(x))$. Moreover since $f(g(x)) = \prod_{i=1}^{n}(g(x)-\beta_i)$, $g(\theta_{ij}) = \beta_i$ for $i = 1, \cdots, n$ and $j = 1, \cdots, m$ are all zeros of $f(g(x))$.

Then any σ in $\mathrm{Gal}\Big(S_{f\circ g}/K\Big)$ maps $\sigma(\theta_{ij}) = \theta_{i'j'}$ for some $1 \le i' \le n$ and $1 \le j' \le m$, thus

$$\beta_{i'} = g(\theta_{i'j'}) = \sigma g(\theta_{ij}) = \sigma(\beta_i) = \beta_i,$$

for the restriction of σ to $K(\beta)$ is identity. Hence $i = i'$, $\sigma(\theta_{ij}) = \theta_{ij'}$, and σ maps a roots of $g(x)-\beta_i$ to another root. Thus $\sigma \in \mathrm{Gal}\Big(g(x) - \beta/K(\beta)\Big)$. □

Let A and B be nonempty disjoint finite sets, and let G and H be permutation groups on A and B respectively. Let H^A be the group of all functions $\{\theta : A \to H\}$ with the canonical multiplication rule, and let A act on H^A by the formula $\theta^a(b) = \theta(a)(b)$ for any $a, b \in A$. Let us define a map on $A \times B$ by,

$$[g, \theta] : A \times B \to A \times B, \quad (a, b) \mapsto \ (g(a), \theta(a)(b)),$$

for $g \in G$ and $\theta \in H^A$. Then $[g,\theta] \in Sym(A \times B)$ and $[g,\theta]$ forms a subgroup of $Sym(A \times B)$. The subgroup of $Sym(A \times B)$ is called the *wreath product* of G by H, and is denoted by $G[H]$.

LEMMA 3.2. [4] *Any element* $[g;\lambda]$ *with* $g \in G$, $\lambda \in H^A$ *satisfies the followings:*

(1) $[g;\lambda](a,b) = \Big(g(a), \lambda(a)b\Big)$ *for* $a \in A$, $b \in B$.

(2) $[g;\lambda][x;\mu](a,b) = [g;\lambda]\Big(x(a), \mu(a)b\Big) = \Big(gx(a), \lambda(x(a))\mu(a)b\Big)$
$= [gx;\lambda(x(a))\mu](a,b)$ *for* $x \in G$, $\mu \in H^A$.

(3) $[g;\lambda]^{-1} = [g^{-1}; \lambda\Big(g^{-1}(a)\Big)^{-1}]$.

(4) $|G[H]| = |G||H|^{|A|}$.

One of the important results about $\mathrm{Gal}\Big(f(g(x))/K\Big)$ is that the Galois group is a wreath product of certain groups ([6]). In the early 1980's, it was asked the Galois group $\mathrm{Gal}\,(f_r(x)/\mathbb{Q})$ of iterate $f_r(x)$ $(r > 0)$ over $\mathbb{Q}$ when $f(x) = x^2 + 1$. It is not hard to see that all $f_r(x)$ are irreducible over the rational. In 1988, Odoni [7] proved that $\mathrm{Gal}\,(f_r(x)/\mathbb{Q})$ is $[C_2]^r$ for $r \leq 750$, where $[C_2]^r = C_2[\cdots[C_2]\cdots]$ denotes the r-fold wreath product of the cyclic group C_2 of order 2 with itself. He gave an algorithm for testing $\mathrm{Gal}\,(f_r(x)/\mathbb{Q}) \cong [C_2]^r$ for any given r. Cremona [1] carried out the algorithm of Odoni up to $r = 5 \cdot 10^7$. He conjectured that $\mathrm{Gal}\,(f_r(x)/\mathbb{Q}) \cong [C_2]^r$ for all r. Moreover for any m-th iteration f_m of f, it was proved that if $f(x) = x^2 - b \in \mathbb{Z}[x]$ then $\mathrm{Gal}\Big(f_m/\mathbb{Q}\Big) \cong [C_2]^m$. And if $f(x) = x^n - b$ with some (minor) conditions then $\mathrm{Gal}\Big(f_m/\mathbb{Q}(\varepsilon_n)\Big) \cong [C_n]^m$. We remark the following lemmas for convenience.

LEMMA 3.3. [2] *Let* K *be a field of characteristic 0 and let* $f(x)$, $g(x) \in K[x]$ *with* $degg(x) = m$. *Assume* $f(g(x))$ *is separable over* K. *Then there is a monomorphism of* $Gal\Big(f(g(x))/K\Big)$ *into* $Gal(f/K)[S_m]$, *where* S_m *is the symmetric* m*-group.*

LEMMA 3.4. [6] *Let* K_0 *be any field,* t_i $(i = 1, \cdots, m)$ *be algebraically independent over* K_0, *and* K *be any extension of* K_0. *Let* $\phi : K_0(t_1, \cdots, t_m) \to K$ *be a* K_0*-algebra morphism, i.e.,* ϕ *is a specialization of parameters, and let* $\tilde{\phi} : K_0(t_1, \cdots, t_m)[x] \to K[x]$ *be the*

induced map from ϕ. If $g(x) \in K_0(t_1, \cdots, t_m)[x]$ where $\tilde{\phi}(g(x))$ is separable over K then $Gal\Big(\tilde{\phi}(g(x))/K\Big)$ is isomorphic to a subgroup of $Gal\Big(g(x)/K_0(t_1, \cdots, t_m)\Big)$.

Lemma 3.4 yields the principle that "Galois groups can not increase under (separable) specialization of parameters."

THEOREM 3.5. *Let K be a field of characteristic 0 and let $f(x)$, $g(x) \in K[x]$ be such that $f(g(x))$ is separable over K. If $f(x)$ is solvable by radical and deg $g(x) < 5$ then $f(g(x))$ is solvable by radical.*

Proof. We may consider an injective homomorphism

$$\phi : \mathrm{Gal}\Big(f(g(x))/K\Big) \to \mathrm{Gal}(f(x)/K)[S_m]$$

due to Lemma 3.3. Since $f(x)$ is solvable by radical, the Galois group $\mathrm{Gal}(f(x)/K)$ is solvable. Moreover S_m is a solvable group for $m < 5$. Since the wreath product of solvable groups is a solvable group ([8], Theorem 2.3.2), the wreath product $\mathrm{Gal}(f(x)/K)[S_m]$ is solvable, and so is its subgroup $\mathrm{Gal}\Big(f(g(x))/K\Big)$. Thus $f(g(x))$ is solvable by radical. □

THEOREM 3.6. *Let K be a field of characteristic 0, t be an indeterminate over K, and let $K(t)$ be the rational function field in one variable t over K. Let $g(x) = x^m + ax + b \in K[x]$ and $\hat{g}(t, x) = x^m + ax + t \in K(t)[x]$. Then $Gal\Big(g(x)/K\Big)$ is isomorphic to a subgroup of $G = Gal\Big(\hat{g}(t, x)/K(t)\Big)$.*

Proof. Let ϕ be a morphism $K(t) \to K$ which maps t to b and $a_i \in K$ to a_i itself, and let $\tilde{\phi} : K(t)[x] \to K[x]$ be the induced map from ϕ. Then $\tilde{\phi}\Big(\hat{g}(t, x)\Big) = g(x)$.

For any $\hat{h}(t, x) = x^r + a_{r-1}x^{r-1} + \cdots + a_1x + t \in K(t)[x]$, it is easy to see that,

$$\tilde{\phi}\Big(\hat{g}(t, x)\hat{h}(t, x)\Big) = \tilde{\phi}\Big(\hat{g}(t, x)\Big)\tilde{\phi}\Big(\hat{h}(t, x)\Big).$$

Thus if $g(x)$ is irreducible over K, then $\hat{g}(t, x)$ is irreducible over $K(t)$. In fact, if $\hat{g}(t, x) = \hat{g}_1(t, x)\hat{g}_2(t, x)$ with non unit $\hat{g}_i \in K(t)[x]$ $(i = 1, 2)$, then

$$g(x) = \tilde{\phi}\Big(\hat{g}(t, x)\Big) = \tilde{\phi}\Big(\hat{g}_1(t, x)\Big)\tilde{\phi}\Big(\hat{g}_2(t, x)\Big)$$

and $\tilde{\phi}(\hat{g}_i(t, x))$ is not unit in $K[x]$.

Moreover if $g(x)$ is separable over K then so is $\hat{g}(t,x)$ over $K(t)$. Indeed, suppose $\hat{g}(t,x) = (x-v_1(t))^{n_1}\cdots(x-v_k(t))^{n_k}$ where we assume that $v_i(t)$ $(t = 1,...,k)$ are distinct polynomials in some splitting field extensions of $K(t)$, and $n_i \geq 1$ with $\sum_{i=1}^{k} n_i = \deg\hat{g} = m$. If we apply $\tilde{\phi}$ to $\hat{g}(t,x)$ then we have

$$g(x) = \tilde{\phi}\Big(\hat{g}(t,x)\Big) = (x-\phi(v_1(t)))^{n_1}\cdots(x-\phi(v_k(t)))^{n_k}$$

in a splitting field extension of K. Since $g(x)$ is separable over K, we have that every $n_i = 1$ and $\phi(v_i(t))$ are distinct in K. Hence we may say every $v_i(t)$ belongs to $K(t)$ and distinct. Thus $\hat{g}(t,x)$ is separable over $K(t)$.

Therefore due to Lemma 3.4, we conclude that

$$\mathrm{Gal}(g(x)/K) = \mathrm{Gal}\Big(\tilde{\phi}(\hat{g}(t,x))/K\Big)$$

is isomorphic to a subgroup of $\mathrm{Gal}\Big(\hat{g}(t,x)/K(t)\Big)$. □

We now turn our attention to polynomials over Hilbertian field. When we say a field K is *Hilbertian*, we mean that for any irreducible polynomial $f(t,x) \in K(t)[x]$ there exist infinitely many $b \in K$ such that the specialization $t \to b \in K$ is defined on $f(t,x)$ and the specialized polynomial $f(b,x)$ is irreducible as a polynomial in $K[x]$.

THEOREM 3.7. *Let the context be as in Theorem 3.6, that is, t is an indeterminate over K, $K(t)$ is the rational function field in one variable t over K. Let $g(x) = x^m + ax + b \in K[x]$ and $\hat{g}(t,x) = x^m + ax + t \in K(t)[x]$. If we assume K is Hilbertian then $Gal\Big(g(x)/K\Big) \cong Gal\Big(\hat{g}(t,x)/K(t)\Big)$.*

Proof. Since K is Hilbertian, if $\hat{g}(t,x)$ is irreducible in $K(t)[x]$ then there is an infinite subset $\Gamma \subset K$ such that for any $u \in \Gamma$, the specialization $\phi : t \mapsto u$ induces $\tilde{\phi}(\hat{g}(t,x))$, which is irreducible in $K[x]$.

Let $\tilde{\phi} :\ K(t)[x] \to K[x]$ be the induced map from ϕ. Without loss of generality, we may consider $b \in \Gamma$, hence $\tilde{\phi}(\hat{g}(t,x)) = \hat{g}(b,x) = g(x)$. Thus the irreducibility of $\hat{g}(t,x)$ over $K(t)$ implies the irreducibility of $g(x)$ over K. Therefore, $\mathrm{Gal}\Big(\hat{g}(t,x)/K\Big) = \mathrm{Gal}\Big(g(x)/K\Big)$. □

References

[1] J. E. Cremona, *On the Galois groups of the iterates of x^2+1*, Mathematika, **36** (1989) 259-261

[2] B. Fein, M. Schacker, *Properties of iterates and composites of polynomials,* J. London Math. Soc. **54** (1996), 489-497
[3] M. Fried, M. Jarden, *Field Arithmetic,* Springer-Verlag, Berlin Heidelberg, 1986
[4] S. Lang, *Algebra,* third edition, Addison-Wesley, Reading, 1993
[5] R. W. K. Odoni, *On the prime divisors of the sequence* $w_{n+1} = 1 + w_1 \dots w_n$, J. London Math. Soc. **32** (1985), no. 2, 1-11
[6] R. W. K. Odoni, *The Galois theory of iterates and composites of polynomials,* Proc. London Math. Soc. **51** (1985), 385-414
[7] R. W. K. Odoni, *Realising wreath products of cyclic groups as Galois groups,* Mathematika, **35** (1988), 101-113
[8] T. Tsuzuku, *Finite groups and finite geometries,* Cambridge University Press, Cambridge, London, 1982

*

Department of Mathematics
Hannam University
Daejeon 133-791, Republic of Korea
E-mail: emc@hnu.kr