JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **24**, No. 4, December 2011

ON IRREDUCIBILITY OF COMPOSITION POLYNOMIALS

EunMi Choi*

Abstract. We investigate the irreducibility of iterate and composite polynomials. For this purpose discriminant and resultant are computed by means of the norm function.

1. Introduction

Let $f_t(x) = (f \circ \cdots \circ f)(x)$ be the t-th iterate of a polynomial $f(x) \in K[x]$. The question whether f_t is factored into irreducible polynomials over a field K is important in determining the Galois group of f_t over K [5]. Discriminant is one of the main tools for solving irreducibility of polynomials. It gives information on whether the roots of f are in K or are in an extension field. As a companion of discriminant, the resultant plays a classical algebraic role for determining whether a system of polynomials have a common root without solving for the roots.

In this paper we investigate the irreducibility of the iterate and composite polynomials. For this purpose we shall compute discriminant and resultant by employing norm functions over fields, and apply the result to determine whether the iterate of a quadratic polynomial is irreducible.

Let $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{j=0}^{m} b_j x^j$ be polynomials over a field K. Let α_i and β_j $(1 \le i \le n; 1 \le j \le m)$ be roots of f and g respectively in some splitting fields over K. The discriminant $\Delta(f)$ and resultant $R(f,g)$ are defined by

$$\Delta(f) = a_n^{2n-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2, \; R(f,g) = a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j).$$

Lemma 1.1. [6] $R(f,g) = a_n^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{nm} b_m^n \prod_{j=1}^{m} f(\beta_j)$. *And* $R(f,f') = (-1)^{n(n-1)/2} a_n \Delta(f)$ *for the derivative* f' *of* f.

Received June 27, 2011; Accepted November 18, 2011.
2010 Mathematics Subject Classification: Primary 11C20, 11R29, 13P15.
Key words and phrases: resultant, iterated polynomial, norm function.

When $\deg f = 2$, f has 2 real roots, a multiple real root, or is irreducible according to $\Delta(f) > 0$, $\Delta(f) = 0$, $\Delta(f) < 0$ respectively. When $\deg f = 3$, f has three distinct real roots if $\Delta(f) > 0$ while f has one real root and two complex conjugate roots if $\Delta(f) < 0$. If $\Delta(f) = 0$ then f may have either one real root of multiplicity 2 and another distinct single real root, or one real root of multiplicity 3. The latter is equivalent to that $R(f, f')$ and $R(f, f'')$ vanish.

In this paper, without mentioned otherwise, we assume $\deg f = n$, $\deg g = m$ with $\mathrm{lc}(f) = a_n$, $\mathrm{lc}(g) = b_m$ where lc stands for the leading coefficient of polynomial.

2. Discriminant of composite polynomials

The computations for resultant and discriminant involve matrix determinant that may be very large size. Though computer computation is largely used recently in this area, we still need to develop effective computation method for these.

LEMMA 2.1. [2] *Let $h(x) \in K[x]$ with $\deg h = t$ and $\mathrm{lc}(h) = c_t$. Then* $R(f \circ h, g \circ h) = \left[c_t^{nm}\ R(f, g)\right]^t$ *and* $R(fh, g) = R(f, g)R(h, g)$.

In this section we shall discuss $\Delta(g \circ f_t)$ in terms of $\Delta(f)$ and $\Delta(g)$.

THEOREM 2.2. *Let γ_i $(1 \le i \le k)$ be all critical points of f. Then*

(1) $\Delta(g \circ f) = (-1)^{\binom{n}{2}m^2} a_n^{m(mn-n-1)} b_m^{n-1} \Delta(g)^n R(g \circ f, f')$
$= (-1)^{\binom{n}{2}m^2} a_n^{m(mn-1)} b_m^{n-1} n^{mn} \Delta(g)^n \prod_{i=1}^k g(f(\gamma_i))$.

(2) $\Delta(g \circ f_2) = a_n^{m(mn^3+mn^2-2n^2-n-1)} b_m^{n^2-1} \Delta(g)^{n^2} R(g \circ f, f')^n R(g \circ f_2, f')$
$= a_n^{m(mn^3+mn^2-n-1)} b_m^{n^2-1} n^{2mn^2} \Delta(g)^{n^2} \prod_{i=1}^k ((g \circ f)^n (g \circ f_2))(\gamma_i)$
$= (-1)^{\binom{n}{2}m^2n^2} a_n^{m(mn^3-n^2-1)} b_m^{n-1} \Delta(g \circ f)^n R(g \circ f_2, f')$.

Proof. Note $\deg(g \circ f) = mn$ and $\mathrm{lc}(g \circ f) = a_n^m b_m$. Since $(g \circ f)' = (g' \circ f) f'$, Lemma 1.1 and 2.1 give rise to

$$\begin{aligned}
& \Delta(g \circ f) = (-1)^{\frac{mn(mn-1)}{2}} (a_n^m b_m)^{-1} R(g \circ f, g' \circ f) R(g \circ f, f') \\
= \ & (-1)^{\frac{mn(mn-1)}{2}} (a_n^m b_m)^{-1} (a_n^{m(m-1)} R(g, g'))^n R(g \circ f, f') \\
= \ & (-1)^{\frac{mn(mn-1)}{2}} a_n^{m(mn-n-1)} b_m^{-1} ((-1)^{\frac{m(m-1)}{2}} b_m \Delta(g))^n R(g \circ f, f') \\
= \ & (-1)^{\binom{n}{2}m^2} a_n^{m(mn-n-1)} b_m^{n-1} \Delta(g)^n R(g \circ f, f'),
\end{aligned}$$

since $\frac{mn(mn-1)}{2} - \frac{mn(m-1)}{2} = \frac{m^2n(n-1)}{2} = \binom{n}{2}m^2$ by considering $(-1)^k = (-1)^{-k}$ for any $k \in \mathbb{Z}$. Moreover since every critical points γ_i of f are

the roots of f',

$$R(g\circ f,f')=(-1)^{mn(n-1)}(na_n)^{mn}\prod_{i=1}^{k}(g\circ f)(\gamma_i)=(na_n)^{mn}\prod_{i=1}^{k}g(f(\gamma_i))$$

for $mn(n-1)$ is even, thus we have

$$\Delta(g\circ f)=(-1)^{\binom{n}{2}m^2}a_n^{m(mn-1)}b_m^{n-1}n^{mn}\Delta(g)^n\prod_{i=1}^{k}g(f(\gamma_i)).$$

Now for $\Delta(g\circ f_2)$, note that $\deg(f_2)=n^2$, $\mathrm{lc}(f_2)=a_n^{n+1}$, $\deg(g\circ f_2)=mn^2$ and $\mathrm{lc}(g\circ f_2)=a_n^{m(n+1)}b_m$. Then

$$\begin{aligned}
&\Delta(g\circ f_2)=(-1)^{\frac{mn^2(mn^2-1)}{2}}(a_n^{m(n+1)}b_m)^{-1}R(g\circ f_2,g'\circ f_2)R(g\circ f_2,f_2')\\
&=(-1)^{\frac{mn^2(mn^2-1)}{2}}(a_n^{m(n+1)}b_m)^{-1}((a_n^{n+1})^{m(m-1)}R(g,g'))^{n^2}R(g\circ f_2,f_2')\\
&=(-1)^{\frac{mn^2(mn^2-1)}{2}}a_n^{m(n+1)(mn^2-n^2-1)}b_m^{-1}R(g,g')^{n^2}R(g\circ f_2,f_2')\\
&=(-1)^{\frac{mn^2(mn^2-1)}{2}}a_n^{m(n+1)(mn^2-n^2-1)}b_m^{-1}\\
&\qquad\cdot((-1)^{\frac{m(m-1)}{2}}b_m\Delta(g))^{n^2}R(g\circ f_2,f_2').
\end{aligned}$$

But $\frac{(mn^2(mn^2-1)-mn^2(m-1))}{2}=\frac{(m^2n^2(n^2-1))}{2}=\binom{n^2}{2}m^2$ is even and

$$R(g\circ f_2,f_2')=(a_n^{mn(n-1)}R(g\circ f,f'))^nR(g\circ f_2,f'),$$

so we have

$$\Delta(g\circ f_2)=a_n^{m(mn^3+mn^2-2n^2-n-1)}b_m^{n^2-1}\Delta(g)^{n^2}R(g\circ f,f')^nR(g\circ f_2,f').$$

Furthermore, with respect to the critical points γ_i of f,

$$\begin{aligned}
&R(g\circ f,f')=(-1)^{mn(n-1)}(na_n)^{mn}\textstyle\prod g\circ f(\gamma_i)=(na_n)^{mn}\prod g\circ f(\gamma_i),\\
&R(g\circ f_2,f')=(-1)^{mn^2(n-1)}(na_n)^{mn^2}\textstyle\prod g\circ f_2(\gamma_i)=(na_n)^{mn^2}\prod g\circ f_2(\gamma_i)
\end{aligned}$$

since $mn(n-1)$ and $mn^2(n-1)$ are even, so

$$\begin{aligned}
\Delta(g\circ f_2)&=a_n^{m(mn^3+mn^2-2n^2-n-1)}b_m^{n^2-1}\Delta(g)^{n^2}\\
&\qquad\cdot((na_n)^{mn}\cdot\textstyle\prod_{i=1}^{k}g\circ f(\gamma_i))^n\cdot(na_n)^{mn^2}\prod_{i=1}^{k}g\circ f_2(\gamma_i)\\
&=a_n^{m(mn^3+mn^2-n-1)}b_m^{n^2-1}n^{2mn^2}\Delta(g)^{n^2}\textstyle\prod_{i=1}^{k}((g\circ f)^n(g\circ f_2))(\gamma_i).
\end{aligned}$$

On the other hand, considering $(g\circ f_2)'$ as $((g\circ f)'\circ f)f'$, we have

$$\begin{aligned}
&\Delta(g\circ f_2)\\
&=(-1)^{\frac{mn^2(mn^2-1)}{2}}(a_n^{m(n+1)}b_m)^{-1}R((g\circ f)\circ f,(g\circ f)'\circ f)R(g\circ f_2,f')\\
&=(-1)^{\frac{mn^2(mn^2-1)}{2}}(a_n^{m(n+1)}b_m)^{-1}(a_n^{mn(mn-1)}R(g\circ f,(g\circ f)'))^nR(g\circ f_2,f')\\
&=(-1)^{\binom{n}{2}m^2n^2}a_n^{m(mn^3-n^2-1)}b_m^{n-1}\Delta(g\circ f)^nR(g\circ f_2,f').
\end{aligned}$$

□

We shall extend this to $\Delta(g\circ f_t)$ for any $t\geq 2$.

THEOREM 2.3. *If γ_i $(1 \le i \le k)$ are critical points of f then*
$\Delta(g\circ f_t) = (-1)^{\binom{n}{2}m^2n^{2(t-1)}} a_n^{m(mn^{2t-1}-n^t-1)} b_m^{n-1}\, \Delta(g\circ f_{t-1})^n\, R(g\circ f_t, f')$
$= (-1)^{\binom{n}{2}m^2n^{2(t-1)}} a_n^{m(mn^{2t-1}-1)} b_m^{n-1} n^{mn^t}\, \Delta(g\circ f_{t-1})^n \prod_{i=1}^k g(f_t(\gamma_i))$.

Proof. We note $\mathrm{lc}(f_t) = a_n \mathrm{lc}(f_{t-1})^n = a_n^{n^{t-1}+\cdots+n+1}$. And $\mathrm{lc}(g\circ f) = b_m \mathrm{lc}(f)^m$ and $\mathrm{lc}(g\circ f_t) = b_m \mathrm{lc}(f_t)^m$. Hence
$\Delta(g\circ f_t) = (-1)^{\frac{mn^t(mn^t-1)}{2}} \mathrm{lc}(g\circ f_t)^{-1} \mathrm{lc}(f)^{mn^t(mn^{t-1}-1)}$
$\cdot\, [(-1)^{\frac{mn^{t-1}(mn^{t-1}-1)}{2}} \mathrm{lc}(g\circ f_{t-1}) \Delta(g\circ f_{t-1})]^n \cdot R(g\circ f_t, f')$.
But since $\frac{1}{2}(mn^t(mn^t - 1 - mn^{t-1} + 1)) = \binom{n}{2} m^2 n^{2(t-1)}$ and
$\mathrm{lc}(g\circ f_t)^{-1} \cdot \mathrm{lc}(f)^{mn^t(mn^{t-1}-1)} \mathrm{lc}(g\circ f_{t-1})^n$
$= (b_m \mathrm{lc}(f_t)^m)^{-1} \mathrm{lc}(f)^{mn^t(mn^{t-1}-1)} (b_m \mathrm{lc}(f_{t-1})^m)^n = b_m^{n-1} a_n^{m(mn^{2t-1}-n^t-1)}$,
we have
$\Delta(g\circ f_t) = (-1)^{\binom{n}{2}m^2n^{2(t-1)}} a_n^{m(mn^{2t-1}-n^t-1)} b_m^{n-1} \Delta(g\circ f_{t-1})^n R(g\circ f_t, f')$.
Moreover since $f'(x) = na_n \prod_{i=1}^k (x - \gamma_i)$, we have
$R(g\circ f_t, f') = (-1)^{mn^t(n-1)} (na_n)^{mn^t} \prod_{i=1}^k g(f_t(\gamma_i))$
$= (na_n)^{mn^t} \prod_{i=1}^k g(f_t(\gamma_i))$,
so it follows that

$$\Delta(g\circ f_t) = (-1)^{\binom{n}{2}m^2n^{2(t-1)}} a_n^{m(mn^{2t-1}-1)} b_m^{n-1} n^{mn^t} \Delta(g\circ f_{t-1})^n \prod_{i=1}^k g(f_t(\gamma_i)).$$

□

3. Discriminant with norm function

Let L/K be a Galois extension and $\alpha \in L$. The norm mapping $N_{L/K} : L \to K$ is defined by $\alpha \mapsto \prod_{\sigma\in \mathrm{Gal}(L/K)} \sigma(\alpha)$, and is useful to reduce elements in the extension field to ground field. We recall a basic property about the norm map.

LEMMA 3.1. [4] *Let $K < E < L$ and $\alpha, \beta \in L$. Then $N_{L/K}(\alpha) = N_{E/K}(N_{L/E}(\alpha))$ and $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha) N_{L/K}(\beta)$. If $\alpha \in K$ then $N_{L/K}(\alpha) = \alpha^{[L:K]}$.*

LEMMA 3.2. *Let $K < L$. If $f = \min_K(\beta) \in K[x]$ is the monic minimal polynomial of $\beta \in L$ of degree n then $\Delta(f) = (-1)^{\binom{n}{2}} \prod_{f(\beta)=0} f'(\beta) = (-1)^{\binom{n}{2}} N_{K(\beta)/K} f'(\beta)$.*

Proof. For the roots $\beta = \beta_1, \beta_2, \cdots, \beta_n$ of f in a splitting field,

$$\Delta(f) = \prod_{i<j}(\beta_i - \beta_j)^2 = (-1)^{\binom{n}{2}} \prod_{i\neq j}(\beta_i - \beta_j) = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} \prod_{i\neq j=1}^{n} (\beta_i - \beta_j).$$

Since $f(x) = \prod_{i=1}^{n}(x - \beta_i)$, we have $f'(x) = \sum_{k=1}^{n} \prod_{k\neq j=1}^{n}(x - \beta_j)$ and

$$f'(\beta_i) = \sum_{k=1}^{n} \prod_{k\neq j=1}^{n} (\beta_i - \beta_j) = \prod_{i\neq j=1}^{n} (\beta_i - \beta_j),$$

thus

$$\Delta(f) = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} f'(\beta_i) = (-1)^{\binom{n}{2}} \prod_{f(\beta)=0} f'(\beta).$$

On the other hand since $|\mathcal{G}| = |\mathrm{Gal}(K(\beta)/K)| = \deg(f) = n$, if σ_i $(1 \leq i \leq n)$ are all elements in $\mathcal{G}$ then $\sigma_i(\beta)$ is one of $\beta_1, \cdots, \beta_n$ thus

$$N_{K(\beta)/K} f'(\beta) = \prod_{\sigma\in\mathcal{G}} \sigma(f'(\beta)) = \prod_{\sigma\in\mathcal{G}} f'(\sigma(\beta)) = \prod_{f(\beta)=0} f'(\beta),$$

hence $\Delta(f) = (-1)^{\binom{n}{2}} N_{K(\beta)/K} f'(\beta)$. □

THEOREM 3.3. *Let $K < L$, $\beta \in L$ and $f, g \in K[x]$. If $g \circ f_t = \min_K(\beta)$ then $g = \min_K(f_t(\beta))$ and $g \circ f_i = \min_K(f_{t-i}(\beta))$ for all $1 \leq i \leq t$. In particular if $f_t = \min_K(\beta) \in K[x]$ then $f_{t-1} = \min_K(f(\beta))$.*

Proof. Assume $g \circ f_t(\beta) = 0$. Write $f_t(\beta) = \alpha_t$ with $g(\alpha_t) = 0$. If $\min_K(\alpha_t) = h(x) \in K[x]$ then $h(x)|g(x)$, and $g = h\tilde{h}$ for some $1 \neq \tilde{h} \in K[x]$. Then

$$0 = g \circ f_t(\beta) = (h\tilde{h}) \circ f_t(\beta) = h(f_t(\beta))\tilde{h}(f_t(\beta)),$$

contradicts to $g \circ f_t = \min_K(\beta)$, so $h = \min_K(\alpha_t) = \min_K(f_t(\beta)) = g$. Moreover for $f_i(\beta) = \alpha_i$ for $1 \leq i \leq t$, it can be seen that

$$\alpha_{i+1} = f(\alpha_i) \text{ and } g \circ f_i(\alpha_{t-i}) = 0 \text{ for all } 1 \leq i < t.$$

If $\min_K(\alpha_{t-i}) = h(x) \in K[x]$ then $h(\alpha_{t-i}) = 0$ and $h|g \circ f_i$, i.e., $g \circ f_i = h\tilde{h}$ for some $1 \neq \tilde{h} \in K[x]$. Then $0 = g \circ f_t(\beta) = g \circ f_i(\alpha_{t-i}) = h\tilde{h}(\alpha_{t-i}) = h(f_{t-i}(\beta))\tilde{h}(f_{t-i}(\beta))$, a contradiction. Thus $h = \min_K(\alpha_{t-i}) = \min_K(f_{t-i}(\beta)) = g \circ f_i$. □

THEOREM 3.4. *Let $\deg f = n$, $L = K(\beta)$ and $f_t = \min_K(\beta)$. Then*

$$\Delta(f_t) = (-1)^{\binom{n}{2} n^{2(t-1)}} \Delta(f_{t-1})^n \prod_{f_t(\beta)=0} f'(\beta).$$

Proof. Note $\deg f_t = n^t$. Lemma 3.2 is the case for $t = 1$ and $f_0 = 1$. Assume $t = 2$. Let $\beta_1 = \beta, \beta_2, \cdots, \beta_{n^2}$ be all roots of $f_2(x)$ in a splitting field. Since $f_2'(x) = f'(f(x))f'(x)$, Lemma 3.1 and 3.2 imply that

$$\Delta(f_2) = (-1)^{\binom{n^2}{2}} N_{L/K} f_2'(\beta) = (-1)^{\binom{n^2}{2}} N_{L/K} f'(f(\beta)) \cdot N_{L/K} f'(\beta).$$

Write $\alpha = f(\beta)$. Due to Theorem 3.3 we may consider $\min_K(\alpha) = f$ and $[K(\alpha) : K] = [L : K(\alpha)] = n$. Hence due to Lemmas 3.1 and 3.2,

$$\begin{aligned} N_{L/K} f'(f(\beta)) &= N_{L/K} f'(\alpha) = N_{K(\alpha)/K}(N_{L/K(\alpha)} f'(\alpha)) \\ &= (N_{K(\alpha)/K} f'(\alpha))^n = ((-1)^{\binom{n}{2}} \Delta(f))^n, \end{aligned}$$

for $f'(\alpha) \in K(\alpha)$. On the other hand any $\sigma \in \mathrm{Gal}(L/K) = \mathcal{G}$ maps β to another zero β_i $(1 \le i \le n^2)$ of $f_2(x)$, so

$$N_{L/K} f'(\beta) = \prod_{\sigma \in \mathcal{G}} f'(\sigma(\beta)) = \prod_{i=1}^{n^2} f'(\beta_i) = \prod_{f_2(\beta)=0} f'(\beta).$$

Therefore

$$\begin{aligned} \Delta(f_2) &= (-1)^{\binom{n^2}{2}} ((-1)^{\binom{n}{2}} \Delta(f))^n \prod_{f_2(\beta)=0} f'(\beta) \\ &= (-1)^{\binom{n}{2} n} \Delta(f)^n \prod_{f_2(\beta)=0} f'(\beta). \end{aligned}$$

Similarly for $t = 3$, we let $f(\beta) = \alpha$ with $f_2(\alpha) = 0$. Then again due to Theorem 3.3, $\min_K(\alpha) = f_2$, $[L : K(\alpha)] = n$ and

$$N_{L/K} f_2'(f(\beta)) = (N_{K(\alpha)/K} f_2'(\alpha))^n = ((-1)^{\binom{n^2}{2}} \Delta(f_2))^n,$$

thus

$$\Delta(f_3) = (-1)^{\binom{n^3}{2}} N_{L/K} f_3'(\beta) = (-1)^{\binom{n^3}{2}} N_{L/K} f_2'(f(\beta)) N_{L/K} f'(\beta)$$

$$= (-1)^{\binom{n^3}{2}} (-1)^{\binom{n^2}{2} n} \Delta(f_2)^n N_{L/K} f'(\beta) = (-1)^{\binom{n}{2} n^4} \Delta(f_2)^n \prod_{f_3(\beta)=0} f'(\beta).$$

Therefore with a root β such that $f_t = \min_K(\beta)$ it follows that

$$\Delta(f_t) = (-1)^{\binom{n}{2} n^{2(t-1)}} \Delta(f_{t-1})^n \prod_{f_t(\beta)=0} f'(\beta).$$

□

We shall generalize this to $\Delta(g \circ f_t)$.

THEOREM 3.5. *Let $L = K(\beta)$ and $g \circ f_t = \min_K(\beta)$ for $f, g \in K[x]$ of degree n, m. Then $\Delta(g \circ f_t) = (-1)^{\binom{n^t}{2}m^2}\Delta(g)^{n^t}\prod_{g\circ f_t(\beta)=0} f_t'(\beta)$.*

Proof. We begin with $t = 1$. Let $\beta = \beta_1, \beta_2, \cdots, \beta_{nm}$ be all roots of $g \circ f$ in a splitting field. Due to Lemma 3.1 and 3.2

$$\Delta(g \circ f) = (-1)^{\binom{mn}{2}} N_{L/K} g'(f(\beta)) \cdot N_{L/K} f'(\beta).$$

If let $f(\beta) = \alpha$ with $g(\alpha) = 0$ then $K < K(\alpha) < L$ with $[L : K] = mn$, $[K(\alpha) : K] = m$, and $\min_K \alpha = g$ by Theorem 3.3. Hence it follows that

$$N_{L/K} g'(f(\beta)) = N_{K(\alpha)/K} g'(\alpha)^n = \left((-1)^{\binom{m}{2}}\Delta(g)\right)^n,$$

while

$$N_{L/K} f'(\beta) = \prod_{\sigma\in\mathcal{G}} \sigma f'(\beta) = \prod_{\sigma\in\mathcal{G}} f'(\sigma(\beta)) = \prod_{i=1}^{mn} f'(\beta_i) = \prod_{g\circ f(\beta)=0} f'(\beta),$$

(here $\mathcal{G} = \mathrm{Gal}(L/K)$), thus we have

$$\begin{aligned}\Delta(g \circ f) &= (-1)^{\binom{mn}{2}}(-1)^{\binom{m}{2}n}\Delta(g)^n \prod_{g\circ f(\beta)=0} f'(\beta) \\ &= (-1)^{\binom{n}{2}m^2}\Delta(g)^n \prod_{g\circ f(\beta)=0} f'(\beta).\end{aligned}$$

Now let $t > 1$ and $f_t(\beta) = \alpha_t$ with $g(\alpha_t) = 0$. Then $g = \min_K(\alpha_t)$ and $K < K(\alpha_t) < L$ with $[L : K(\alpha_t)] = n^t$, $[K(\alpha_t) : K] = m$. Since

$N_{L/K} g'(f_t(\beta)) = (N_{K(\alpha_t)/K} g'(\alpha_t))^{n^t} = \left((-1)^{\binom{m}{2}}\Delta(g)\right)^{n^t}$

and

$N_{L/K} f_t'(\beta) = \prod_{\sigma\in\mathcal{G}} \sigma(f_t'(\beta)) = \prod_{\sigma\in\mathcal{G}} f_t'(\sigma(\beta)) = \prod_{g\circ f_t(\beta)=0} f_t'(\beta)$,

it follows from Lemma 3.2 that

$$\begin{aligned}\Delta(g \circ f_t) &= (-1)^{\binom{mn^t}{2}} N_{L/K} g'(f_t(\beta)) N_{L/K} f_t'(\beta) \\ &= (-1)^{\binom{mn^t}{2}}((-1)^{\binom{m}{2}}\Delta(g))^{n^t} \prod_{g\circ f_t(\beta)=0} f_t'(\beta) \\ &= (-1)^{\binom{n^t}{2}m^2}\Delta(g)^{n^t} \prod_{g\circ f_t(\beta)=0} f_t'(\beta).\end{aligned}$$

□

4. Discriminant of composition with norm function

In this section we shall investigate $N_{L/K}f_t'(\beta)$ explicitly in order express $\Delta(g\circ f_t)$ by $f'(\beta)$ not by $f_t'(\beta)$.

LEMMA 4.1. *With the same context in Theorem 3.5, for* $1\le i<t$,

$$N_{K(\alpha_{t-i})/K}f'(\alpha_{t-i}) = (-1)^{\binom{n}{2}m^2n^{2(i-1)}}\Delta(g\circ f_{i-1})^{-n}\Delta(g\circ f_i).$$

Proof. Note that $f_0=1$. From $f_i(\beta)=\alpha_i$, $\alpha_{i+1}=f(\alpha_i)$ $(1\le i<t)$ due to Theorem 3.5. Clearly $K<K(\alpha_t)<\cdots<K(\alpha_1)<K(\beta)=L$, and $[L:K(\alpha_1)]\le n$ and $[K(\alpha_i):K(\alpha_{i+1})]\le n$ for $1\le i<t$. But since

$$n^t=[L:K(\alpha_t)]=[L:K(\alpha_1)][K(\alpha_1):K(\alpha_2)]\cdots[K(\alpha_{t-1}):K(\alpha_t)]\le n^t,$$

we have $[L:K(\alpha_1)]=[K(\alpha_i):K(\alpha_{i+1})]=n$ for $1\le i<t$. Moreover α_i are zeros of $g\circ f_{t-i}$ and $\min_K\alpha_i=g\circ f_{t-i}$, thus

$$[K(\alpha_t):K]=m=\deg(g),\quad [K(\alpha_{t-i}):K]=mn^{t-i}=\deg(g\circ f_{t-i}),$$

and $[L:K]=\deg(g\circ f_t)$. So $N_{K(\alpha_t)/K}g'(\alpha_t)=(-1)^{\binom{m}{2}}\Delta(g)$ and

$$\begin{aligned}
&(-1)^{\binom{mn}{2}}\Delta(g\circ f) = N_{K(\alpha_{t-1})/K}g'(f(\alpha_{t-1}))\cdot N_{K(\alpha_{t-1})/K}f'(\alpha_{t-1})\\
=\;& N_{K(\alpha_{t-1})/K}g'(\alpha_t)\cdot N_{K(\alpha_{t-1})/K}f'(\alpha_{t-1})\\
=\;& N_{K(\alpha_t)/K}N_{K(\alpha_{t-1})/K(\alpha_t)}g'(\alpha_t)\cdot N_{K(\alpha_{t-1})/K}f'(\alpha_{t-1})\\
=\;& \left(N_{K(\alpha_t)/K}g'(\alpha_t)\right)^n\cdot N_{K(\alpha_{t-1})/K}f'(\alpha_{t-1})\\
=\;& ((-1)^{\binom{m}{2}}\Delta(g))^n\cdot N_{K(\alpha_{t-1})/K}f'(\alpha_{t-1}),
\end{aligned}$$

so

$$\begin{aligned}
N_{K(\alpha_{t-1})/K}f'(\alpha_{t-1}) &= (-1)^{\binom{mn}{2}-\binom{m}{2}n}\Delta(g)^{-n}\Delta(g\circ f)\\
&= (-1)^{\binom{n}{2}m^2}\Delta(g)^{-n}\Delta(g\circ f).
\end{aligned}$$

Similar to this,

$$\begin{aligned}
&(-1)^{\binom{mn^2}{2}}\Delta(g\circ f_2) = N_{K(\alpha_{t-2})/K}g'(f_2(\alpha_{t-2}))N_{K(\alpha_{t-2})/K}f_2'(\alpha_{t-2})\\
=\;& N_{K(\alpha_{t-2})/K}g'(f(\alpha_{t-1}))N_{K(\alpha_{t-2})/K}f'(f(\alpha_{t-2}))N_{K(\alpha_{t-2})/K}f'(\alpha_{t-2})\\
=\;& N_{K(\alpha_{t-2})/K}g'(\alpha_t)N_{K(\alpha_{t-2})/K}f'(\alpha_{t-1})N_{K(\alpha_{t-2})/K}f'(\alpha_{t-2})\\
=\;& \left(N_{K(\alpha_t)/K}g'(\alpha_t)\right)^{n^2}\left(N_{K(\alpha_{t-1})/K}f'(\alpha_{t-1})\right)^n N_{K(\alpha_{t-2})/K}f'(\alpha_{t-2})\\
=\;& ((-1)^{\binom{m}{2}}\Delta(g))^{n^2}((-1)^{\binom{n}{2}m^2}\Delta(g)^{-n}\Delta(g\circ f))^n N_{K(\alpha_{t-2})/K}f'(\alpha_{t-2})
\end{aligned}$$

thus

$$\begin{aligned}
N_{K(\alpha_{t-2})/K}f'(\alpha_{t-2}) &= (-1)^{\binom{mn^2}{2}-\binom{m}{2}n^2-\binom{n}{2}m^2n}\Delta(g\circ f)^{-n}\Delta(g\circ f_2)\\
&= (-1)^{\binom{n}{2}m^2n^2}\Delta(g\circ f)^{-n}\Delta(g\circ f_2).
\end{aligned}$$

Furthermore since

$$(g\circ f_3)'(\alpha_{t-3}) = g'(f_3(\alpha_{t-3}))f_3'(\alpha_{t-3}) = g'(\alpha_t)f_2'(f(\alpha_{t-3}))f'(\alpha_{t-3})$$
$$= g'(\alpha_t)f_2'(\alpha_{t-2})f'(\alpha_{t-3}) = \cdots = g'(\alpha_t)\prod_{i=1}^{3} f'(\alpha_{t-i})$$

we have

$$(-1)^{\binom{mn^3}{2}}\Delta(g\circ f_3) = N_{K(\alpha_{t-3})/K}g'(\alpha_t)\ \prod_{i=1}^{3} N_{K(\alpha_{t-3})/K}f'(\alpha_{t-i})$$
$$= \left((-1)^{\binom{m}{2}}\Delta(g)\right)^{n^3}\left((-1)^{\binom{n}{2}m^2}\Delta(g)^{-n}\Delta(g\circ f)\right)^{n^2}$$
$$\left((-1)^{\binom{n}{2}m^2n^2}\Delta(g\circ f)^{-n}\Delta(g\circ f_2)\right)^{n} N_{K(\alpha_{t-3})/K}f'(\alpha_{t-3}),$$

thus

$$N_{K(\alpha_{t-3})/K}f'(\alpha_{t-3})$$
$$= (-1)^{\binom{mn^3}{2}-\binom{m}{2}n^3-\binom{n}{2}m^2n^2-\binom{n}{2}m^2n^3}\Delta(g\circ f_2)^{-n}\Delta(g\circ f_3)$$
$$= (-1)^{\binom{n}{2}m^2n^4}\Delta(g\circ f_2)^{-n}\Delta(g\circ f_3).$$

Continually, for $1\le i<t$, we have

$$N_{K(\alpha_{t-i})/K}f'(\alpha_{t-i}) = (-1)^{\binom{n}{2}m^2n^{2(i-1)}}\Delta(g\circ f_{i-1})^{-n}\Delta(g\circ f_i).$$

□

THEOREM 4.2. *With the same context in Theorem 3.5,*

$$\Delta(g\circ f_t) = (-1)^{\binom{n}{2}m^2n^{2(t-1)}}N_{L/K}f'(\beta)\Delta(g\circ f_{t-1})^n.$$

Proof. We keep the same notations as above. Since

$$f_t'(\beta) = f_{t-1}'(f(\beta))\ f'(\beta) = f_{t-2}'(f(\alpha_1))\ f'(\alpha_1)\ f'(\beta)$$
$$= f'(\alpha_{t-1})\ f'(\alpha_{t-2})\cdots f'(\alpha_2)\ f'(\alpha_1)\ f'(\beta) = f'(\beta)\prod_{i=1}^{t-1} f'(\alpha_i)$$

we have

$$N_{L/K}f_t'(\beta) = N_{L/K}f'(\beta)\prod_{i=1}^{t-1} N_{K(\alpha_i)/K}N_{L/K(\alpha_i)}f'(\alpha_i)$$
$$= N_{L/K}f'(\beta)\prod_{i=1}^{t-1}(N_{K(\alpha_i)/K}f'(\alpha_i))^{n^i}$$
$$= N_{L/K}f'(\beta)\prod_{i=1}^{t-1}((-1)^{\binom{n}{2}m^2n^{2(t-i-1)}}\Delta(g\circ f_{t-i-1})^{-n}\Delta(g\circ f_{t-i}))^{n^i}$$

$$= \quad (-1)^{\binom{n^{t-1}}{2}m^2n} \cdot N_{L/K}f'(\beta)\ \Delta(g\circ f_{t-1})^n\Delta(g)^{-n^t}$$

Hence together with Theorem 3.5, we have

$$\begin{aligned}
&\Delta(g\circ f_t) = (-1)^{\binom{mn^t}{2}}N_{L/K}g'(f_t(\beta))\cdot N_{L/K}f_t'(\beta)\\
= \quad &(-1)^{\binom{mn^t}{2}}(-1)^{\binom{m}{2}n^t}\Delta(g)^{n^t}(-1)^{\binom{n^{t-1}}{2}m^2n}\\
&\cdot N_{L/K}f'(\beta)\Delta(g\circ f_{t-1})^n\Delta(g)^{-n^t}\\
= \quad &(-1)^{\binom{mn^t}{2}}(-1)^{\binom{m}{2}n^t}(-1)^{\binom{n^{t-1}}{2}m^2n}\cdot N_{L/K}f'(\beta)\Delta(g\circ f_{t-1})^n
\end{aligned}$$

By considering $(-1)^k = (-1)^{-k}$ for any $k\in\mathbb{Z}$, since

$$\binom{mn^t}{2} - \binom{m}{2}n^t - \binom{n^{t-1}}{2}m^2n = m^2n^{2(t-1)}\frac{n(n-1)}{2} = \binom{n}{2}m^2n^{2(t-1)},$$

we conclude that

$$\Delta(g\circ f_t) = (-1)^{\binom{n}{2}m^2n^{2(t-1)}}N_{L/K}f'(\beta)\Delta(g\circ f_{t-1})^n.$$

□

5. Irreducibility of composite polynomials

If β is a root of $g(x)$ and θ is a root of $f(x)-\beta$ then θ is a root of $g\circ f$. On the other hand if α_i are roots of $g\circ f$ then $f(\alpha_i)$ gives the zeros of $g(x)$ so the splitting field of f is contained in the splitting field of $g\circ f$. Thus if β be a root of $g(x)$ then every root of $f(x)-\beta$ is a root of $g(f(x))$. Conversely if α is a root of $g\circ f$ then $f(\alpha)$ is a root of $g(x)$.

Lemma 5.1. [3] *$g\circ f$ is irreducible in $K[x]$ if and only if g is irreducible in $K[x]$ and $f-\beta$ is irreducible in $K(\beta)[x]$ for every root β of $g(x)$.*

Theorem 5.2. *Assume $f(x)=ax^2+bx+c$ and $g\circ f_{t-1}$ is irreducible over K for $t\geq 2$. Then $g\circ f_t$ is irreducible over K if one of the following holds.*

(1) $N_{K(\sqrt{\Delta(h)})/K}\sqrt{\Delta(h)}\notin K^2$ *for* $g\circ f_{t-1}(\beta)=0$ *and* $h(x)=f(x)-\beta\in K(\beta)[x]$.
(2) $g\circ f_t(\gamma)\notin K^2$ *for the critical point* γ *of* f.

Proof. Because $g\circ f_{t-1}$ is irreducible over K, $g\circ f_t=(g\circ f_{t-1})\circ f$ is irreducible over K if and only if $f(x)-\beta$ is irreducible over $K(\beta)$ for any root β of $g\circ f_{t-1}$. Let $h=f-\beta\in K(\beta)[x]$. Then h is irreducible over $K(\beta)$ is equivalent to that the zeros of $h(x)$ are not belong to $K(\beta)$,

i.e. $\Delta(h) = -4a(-\frac{b^2}{4a} + c - \beta)$ is not in $K(\beta)^2$. Thus $g \circ f_t$ is irreducible over K if, at least, the norm $N_{K(\beta)/K}(\Delta(h))$ is not in K^2. Now

$$\begin{aligned} N_{K(\beta)/K}\Delta(f-\beta) &= N_{K(\beta)/K}(-4a)N_{K(\beta)/K}(-\frac{b^2}{4a}+c-\beta) \\ &= (-4a)^{m2^{t-1}} \prod_{\sigma\in \mathrm{Gal}(K(\beta)/K)} \sigma(-\frac{b^2}{4a}+c-\beta) \end{aligned}$$

for $[K(\beta) : K] = \deg(g \circ f_{t-1}) = m2^{t-1}$. Every σ maps β to another root β_i of $g \circ f_{t-1}$ $(1 \le i \le m2^{t-1})$ with $\beta = \beta_1$ and leaves K fixed, so

$$\begin{aligned} & N_{K(\beta)/K}(\Delta(f-\beta)) \\ = \ & (4a)^{m2^{t-1}}(-\frac{b^2}{4a}+c-\beta_1)(-\frac{b^2}{4a}+c-\beta_2)\cdots(-\frac{b^2}{4a}+c-\beta_{m2^{t-1}}) \\ = \ & (4a)^{m2^{t-1}} \prod_{i=1}^{m2^{t-1}} (-\frac{b^2}{4a}+c-\beta_i) = (4a)^{m2^{t-1}} \prod_{g\circ f_{t-1}(\beta)=0} (f(\gamma)-\beta) \end{aligned}$$

since $-\frac{b^2}{4a} + c = f(-\frac{b}{2a}) = f(\gamma)$ with the critical point $\gamma = -\frac{b}{2a}$ of f.

We note that, in some large enough extension field of K, we can write $f(x) = \prod_{f(\omega)=0}(x - \omega)$. Similar to this

$$g \circ f(x) = \prod_{g(\omega)=0} (f(x) - \omega) \text{ and } g \circ f_t(x) = \prod_{g\circ f_{t-1}(\omega)=0} (f(x) - \omega).$$

But since $g \circ f_{t-1}(\beta_i) = 0$ for $1 \le i \le m2^{t-1}$,

$$g \circ f_t(x) = \prod_{g\circ f_{t-1}(\beta)=0} (f(x) - \beta)$$

so

$$N_{K(\beta)/K}(\Delta(f-\beta)) = (4a)^{m2^{t-1}}(g \circ f_t)(\gamma).$$

If $(4a)^{m2^{t-1}} g \circ f_t(\gamma) \notin K^2$, i.e., $g \circ f_t(-\frac{b}{2a}) \notin K^2$ then $g \circ f_t$ is irreducible over K. □

Corollary 5.3. *Let $f(x) = ax^2 + bx + c$. If f_{t-1} is irreducible for some $t \ge 2$ and $f_t(-\frac{b}{2a})$ is not a square in K then f_t is irreducible.*

Proof. f_t is irreducible over K if and only if $f(x) - \beta$ is irreducible over $K(\beta)$ for any root β of f_{t-1}, that is, $b^2 - 4ac + 4a\beta$ is not a square in $K(\beta)$. Since

$$N_{K(\beta)/K}(b^2 - 4ac + 4a\beta) = (-4a)^{2^{t-1}} \prod_{f^{t-1}(\beta)=0} (-\frac{b^2}{4a} + c) - \beta$$

$$= (4a)^{2^{t-1}} f_{t-1}(-\frac{b^2}{4a} + c) = (4a)^{2^{t-1}} f_{t-1}(f(-\frac{b}{2a})),$$

if $f_t(-\frac{b}{2a}) = f_{t-1}f(-\frac{b}{2a}) = N_{K(\beta)/K}(b^2 - 4ac + 4a\beta)$ is not a square in K then $(b^2 - 4ac + 4a\beta)$ is not in $K(\beta)^2$, so f_t is irreducible over K. □

References

[1] R. Jones, *The density of prime divisors in the arithmetic dynamics of quadratic polynomials*, J. London Math. Soc. (2), **78** (2008), no. 2, 523-544.

[2] J. H. McKay, S. S. Wang. *A chain rule for the resultant of two polynomials*, Arch. Math. **53** (4). (1989) 347-351.

[3] R. K. W. Odoni, *The Galois theory of iterates and composites of polynomials*, Prod. London Math Soc. (3), **51** (1985), no. 3, 385-414.

[4] J. R. Bastida, *Field extensions and Galois theory*, Encyclopedia of Mathematics and its applications, 22, Addison-Wesley Publishing Company, 1984.

[5] R. G. Swan, *Factorization of polynomials over finite field*, Pacific Journal of Mathematics **12** (1962), 1099-1106.

[6] J. J. Sylvester, *On a general method of determining by mere inspection the derivation from two equations of any degree*, Philosophical Magazine **16** (1840), 132-135.

*

Department of Mathematics
HanNam University
Daejeon 306-791, Republic of Korea
E-mail: emc@hnu.kr