Honam Mathematical J. **33** (2011), No. 3, pp. 355–366
http://dx.doi.org/10.5831/HMJ.2011.33.3.355

# IRREDUCIBLE POLYNOMIALS WITH REDUCIBLE COMPOSITIONS

Eunmi Choi

**Abstract.** In this paper we investigate criteria that for an irreducible monic quadratic polynomial $f(x) \in \mathbb{Q}[x]$, $f \circ g$ is reducible over $\mathbb{Q}$ for an irreducible polynomial $g(x) \in \mathbb{Q}[x]$. Odoni intrigued the discussion about an explicit form of irreducible polynomials $f(x)$ such that $f \circ f$ is reducible. We construct a system of infinitely many such polynomials.

## 1. Introduction

For a field $K$ with char.0, let $f(x)$ and $g(x)$ be in $K[x]$. Then $f \circ g$ is irreducible in $K[x]$ if and only if $f(x)$ is irreducible in $K[x]$ and $g(x) - \alpha$ is irreducible in $K(\alpha)[x]$ for every root $\alpha$ of $f(x)$. This is a well known property for the irreducibility of $f \circ g$ due to Capelli (refer to [4], [2]). In particular if $f(x) = x^2 - bx + c$ is a monic quadratic polynomial then the next lemma follows immediately.

**Lemma 1.** *If $f(x) = x^2 - bx + c$ is irreducible in $K[x]$ with discriminant $\Delta$, then for any polynomial $g(x) \in K[x]$, $f \circ g$ is reducible over $K$ if and only if $g(x) - \alpha = g(x) - \frac{b}{2} - \sqrt{\frac{\Delta}{4}}$ is reducible over $K(\alpha) = K(\sqrt{\frac{\Delta}{4}})$.*

The purpose of this paper is to construct irreducible quadratic polynomials $f(x) = x^2 - bx + c \in \mathbb{Q}[x]$ explicitly such that the composition of itself is reducible. We also investigate irreducible polynomials $f$ and $g$ while $f \circ g$ is reducible.

Throughout the paper, without mentioned otherwise, we keep notations that $f(x) = x^2 - bx + c$, $\alpha$ is a root of $f(x)$ in some splitting field,

---

Received June 28, 2011. Accepted July 16, 2011.
2000 Mathematics Subject Classification. 11D09, 12F10, 20B05.
Key words and phrases. Resultant, Discriminant, Iterated polynomial.
This paper was supported by Hannam University Research Fund 2011.

$\Delta$ is the discriminant of $f$ and $\Delta_0 = \frac{\Delta}{4}$. Then $\alpha = \frac{1}{2}(b + \sqrt{b^2 - 4c}) = \frac{b}{2} + \frac{\sqrt{\Delta}}{2} = \frac{b}{2} + \sqrt{\Delta_0}$.

## 2. Irreducible polynomial with reducible iterate

In [3], it is given as an explicit example that $f(x) = x^2 + 10x + 17$ is irreducible over $\mathbb{Q}$ but $f \circ f$ is reducible over $\mathbb{Q}$. In this section we shall develop certain criterion in order to construct an infinite series of such polynomials.

**Theorem 2.** *Let $f(x) = x^2 - bx + c \in \mathbb{Q}[x]$ $(b \neq 0)$ be an irreducible monic polynomial. Let $U = \sqrt{(\Delta + 2b)^2 - 4\Delta}$.*
*If $c = \frac{1}{4}\left(b^2 + 2b - 2 \pm \sqrt{-8b + 4 + U^2}\right)$ and $\frac{1}{2}(\Delta + 2b \pm U) \in \mathbb{Q}^2$ then $f \circ f$ is reducible.*

**Proof.** Due to Lemma 1, $f \circ f$ is reducible if and only if $f(x) - \alpha$ is reducible over $\mathbb{Q}(\alpha)$, i.e., the discriminant $\Delta(f(x) - \alpha)$ belongs to $\mathbb{Q}(\alpha)^2 = \mathbb{Q}(\sqrt{\Delta})^2$. Moreover since $f(x) - \alpha = x^2 - bx + c - \frac{b}{2} - \frac{\sqrt{\Delta}}{2}$,

$$\Delta(f(x) - \alpha) = b^2 - 4c + 2b + 2\sqrt{\Delta} = \Delta + 2b + 2\sqrt{\Delta} \in \mathbb{Q}(\sqrt{\Delta})^2$$

so we may write $\Delta + 2b + 2\sqrt{\Delta} = (s + t\sqrt{\Delta})^2$ for some $s, t \in \mathbb{Q}$. Then

$$\Delta + 2b = s^2 + t^2\Delta \quad \text{and} \quad st = 1.$$

Hence $t = \frac{1}{s}$ and $\Delta + 2b = s^2 + \frac{\Delta}{s^2}$. Thus we have a quartic polynomial on $s$ that $s^4 - (\Delta + 2b)s^2 + \Delta = 0$ so

$$s^2 = \frac{1}{2}\left(\Delta + 2b \pm \sqrt{(\Delta + 2b)^2 - 4\Delta}\right).$$

If $(\Delta+2b)^2 - 4\Delta = 0$ then $\Delta = \left(\frac{\Delta+2b}{2}\right)^2$. If $\Delta + 2b = 0$ then $0 = \Delta = -2b$, it contradicts to $b \neq 0$. Hence $\Delta + 2b \neq 0$ so $\Delta = \left(\frac{\Delta+2b}{2}\right)^2 \neq 0$ yields $f$ is reducible, contradict. Thus we may have

$$(\Delta + 2b)^2 - 4\Delta = U^2 \text{ and } s^2 = \frac{1}{2}(\Delta + 2b \pm U)$$

for some $0 \neq U \in \mathbb{Q}$. Moreover since

$$U^2 = (\Delta + 2b)^2 - 4\Delta = 16c^2 - 8(b^2 + 2b - 2)c + (b^4 + 4b^3),$$

we have $c^2 - \frac{1}{2}(b^2 + 2b - 2)c + \frac{1}{16}(b^4 + 4b^3 - U^2) = 0$, so

$$c = \frac{1}{2}\Big(\frac{1}{2}(b^2 + 2b - 2) \pm \sqrt{\frac{1}{4}(b^2 + 2b - 2)^2 - \frac{1}{4}(b^4 + 4b^3 - U^2)}\Big)$$

$$= \frac{1}{4}(b^2 + 2b - 2 \pm \sqrt{-8b + 4 + U^2})$$

where $-8b + 4 + U^2 \in \mathbb{Q}^2$. Thus by taking $c$ as above we can construct $f(x)$ such that $f \circ f$ is reducible. □

The polynomial $f(x) = x^2 + 10x + 17$ in [3] meets the necessary conditions in Theorem 2. In fact since $\Delta(f) = 2^5$,

$$U^2 = (\Delta + 2b)^2 - 4\Delta = 2^4 \text{ and } s^2 = \frac{1}{2}(\Delta + 2b - U) = 2^2$$

are squares of integers. We note that here we take $s^2 = \frac{1}{2}(\Delta + 2b - U)$ instead of $s^2 = \frac{1}{2}(\Delta + 2b + U)$. Hence $f \circ f$ is should be reducible. Indeed

$$f \circ f(x) = x^4 + 20x^3 + 144x^2 + 440x + 476 = (x^2 + 12x + 34)(x^2 + 8x + 14).$$

Due to Theorem 2, we are able to construct infinitely many irreducible polynomials $f(x)$ that its iterate $f \circ f$ is reducible. We will find a system of such polynomials precisely in two cases that $-8b + 4 + U^2 = 0$ or $-8b + 4 + U^2 \in \mathbb{Q}^2$.

Example 1. Assume $-8b + 4 + U^2 = 0$. Then $c = \frac{1}{4}(b^2 + 2b - 2)$. Since $U^2 = 8b - 4 > 0$, it should be $b > 2$. Thus for the $b, c, U, s \in \mathbb{Q}$ with

$$b > 2,\ U^2 = 8b - 4,\ s^2 = \frac{1}{2}(\Delta + 2b \pm U),$$

we can construct a family of polynomials $f(x) = x^2 - bx + c$ which are irreducible but the 2nd iterate are reducible. Indeed we have some examples as follows:

| $b > 2$ | $8b - 4 = U^2$ | $c = \frac{b^2+2b-2}{4}$ | $\Delta = -2b + 2$ | $\frac{\Delta+2b\pm U}{2} = s^2$ |
|---|---|---|---|---|
| (1) 5 | $6^2$ | 33/4 | −8 | $2^2$ |
| (2) 113 | $30^2$ | 12993/4 | −224 | $4^2$ |
| (3) 613 | $70^2$ | 376993/4 | −1224 | $6^2$ |
| (4) 1985 | $126^2$ | 3944193/4 | −3968 | $8^2$ |
| ... | | | | |

In the case (1), let $b = 5$. Then $c = 33/4$ so $f(x) = x^2 - 5x + \frac{33}{4}$ is irreducible since $\Delta = -8 < 0$, but the composition $f \circ f$ is reducible that

$f \circ f(x) = x^4 - 10x^3 + \frac{73}{2}x^2 - \frac{115}{2}x + \frac{561}{16} = \frac{1}{16}(4x^2 - 12x + 11)(4x^2 - 28x + 51)$.

Similarly in (2) by taking $b = 113$, we have $f(x) = x^2 - 113x + \frac{12993}{4}$ which is irreducible but reducible composition

$f \circ f(x) = x^4 - 226x^3 + \frac{38305}{2}x^2 - \frac{1442671}{2}x + \frac{162997185}{16}$

$= \frac{1}{16}(4x^2 - 463x + 11895)(4x^2 - 468x + 13703)$.
(3) shows that $f(x) = x^2 - 613x + \frac{376993}{4}$ is irreducible and
$f \circ f(x) = x^4 - 1226x^3 + \frac{1127305}{2}x^2 - \frac{230345171}{2}x + \frac{141200843185}{16}$
$= \frac{1}{16}(4x^2 - 2428x + 368483)(4x^2 - 2476x + 383195)$.
And in (4), $f(x) = x^2 - 1985x + \frac{3944193}{4}$ is irreducible and
$f \circ f(x) = \frac{1}{16}(4x^2 - 7908x + 3908591)(4x^2 - 7972x + 3972111)$.

Besides these examples we can construct infinitely many polynomials satisfying the conditions on $c$ and $U$, which are irreducible with reducible 2nd iterate.

Example 2. Assume $-8b + 4 + U^2 = V^2$ for some $V \in \mathbb{Q}$. Then $8b - 4 = (U + V)(U - V) > 0$ and $c = \frac{1}{4}(b^2 + 2b - 2 + V)$. Thus

$$s^2 = \frac{1}{2}(\Delta + 2b + U) = \frac{1}{2}\left(b^2 - 4c + 2b + U\right) = \frac{1}{2}(2 + U - V),$$

so $U - V = 2(s^2 - 1)$. Now for $c$, $U$, $V$ satisfying

$$8b - 4 = (U + V)(U - V),\ U - V = 2(s^2 - 1),$$

$$c = \frac{1}{4}(b^2 + 2b - 2 + V),\ s^2 = \frac{1}{2}(\Delta + 2b + U) \text{ and } -2b + 2 < V,$$

we can construct series of $f(x) = x^2 - bx + c$ which are irreducible but the 2nd iterate are reducible.

| $b > 2$ | $8b - 4 = (U - V)(U + V)$ | $U - V = 2(s^2 - 1)$ | $s^2$ | $U + V$ | $U$ | $V$ |
|---|---|---|---|---|---|---|
| (1) 8 | $(2^2)(3)(5)$ | $(2)(3) = 2(2^2 - 1)$ | $2^2$ | 10 | 8 | 2 |
| (2) 11 | $(2^2)(3)(7)$ | $(2)(3) = 2(2^2 - 1)$ | $2^2$ | 14 | 10 | 4 |
| (3) 14 | $(2^2)(3^3)$ | $(2)(3) = 2(2^2 - 1)$ | $2^2$ | 18 | 12 | 6 |
| (4) 17 | $(2^2)(3)(11)$ | $(2)(3) = 2(2^2 - 1)$ | $2^2$ | 22 | 14 | 8 |
| (5) 20 | $(2^2)(3)(13)$ | $(2)(3) = 2(2^2 - 1)$ | $2^2$ | 26 | 16 | 10 |
| $\cdots$ | | | | | | |

In case (1), let $b = 8$. Then $c = (b^2 + 2b - 2 + V)/4 = 20$ and $\Delta = -16 < 0$, so

$$s^2 - \frac{1}{2}(\Delta + 2b + U) = 2^2 - \frac{1}{2}(-16 + 16 + 8) = 0$$

as is expected. Thus $f(x) = x^2 - 8x + 20$ is irreducible but
$f \circ f(x) = x^4 - 16x^3 + 96x^2 - 256x + 260 = (x^2 - 10x + 26)(x^2 - 6x + 10)$ is reducible. In (2), let $b = 11$. Then $c = 145/4$ and $\Delta = -24 < 0$, so

$$s^2 - \frac{1}{2}(\Delta + 2b \pm U) = 2^2 - \frac{1}{2}(-24 + 22 + 10) = 0$$

as is expected. Hence we have an irreducible $f(x) = x^2 - 11x + 145/4$ with

$f \circ f(x) = x^4 - 22x^3 + \frac{365}{2}x^2 - 13 = \frac{1}{16}(4x^2 - 52x + 175)(4x^2 - 36x + 87)$.
Similarly in (3), $b = 14$, $c = 57$ and $\Delta = -32 < 0$, so

$$s^2 - \frac{1}{2}(\Delta + 2b \pm U) = 2^2 - \frac{1}{2}(-32 + 28 + 12) = 0.$$

So we have an irreducible polynomial $f(x) = x^2 - 14x + 57$ such that $f \circ f(x) = x^4 - 28x^3 + 296x^2 - 1400x + 2508 = (x^2 - 12x + 38)(x^2 - 16x + 66)$. And in case (4), $b = 17$, $c = 329/4$ and $\Delta = -40 < 0$, so

$$s^2 - \frac{1}{2}(\Delta + 2b \pm U) = 2^2 - \frac{1}{2}(-40 + 34 + 14) = 0,$$

thus $f(x) = x^2 - 17x + 329/4$ is an irreducible polynomial such that

$$f \circ f(x) = \frac{1}{16}(4x^2 - 60x + 235)(4x^2 - 76x + 371).$$

For (5), $b = 20$, $c = 112$ and $\Delta = -48 < 0$, so

$$s^2 - \frac{1}{2}(\Delta + 2b \pm U) = 2^2 - \frac{1}{2}(-48 + 40 + 16) = 0,$$

and $f(x) = x^2 - 20x + 112$ is an irreducible polynomial such that

$$f \circ f(x) = (x^2 - 22x + 124)(x^2 - 18x + 84).$$

Therefore besides the polynomial $x^2 + 10x + 17$ in [3], we can construct infinitely many quadratic irreducible polynomials whose 2nd iterate are reducible.

## 3. Irreducible polynomial with reducible composition

This section is devoted to investigate the nature of irreducible quadratic polynomial $f$ such that the composition $f \circ g$ is reducible while $g(x)$ is irreducible of any degree. Let $f(x) = ax^2 - bx + c$ with a root $\alpha = \frac{b}{2a} + \sqrt{\Delta_0}$ for $\Delta_0 = \frac{\Delta}{4a^2}$.

**Lemma 3.** *Let $f(x) = ax^2 - bx + c$ be irreducible. Then for any $g(x) \in K[x]$, $f \circ g$ is reducible over $K$ if and only if*

$$\begin{cases} g(x) - \frac{b}{2a} & = A(x)U(x) + \Delta_0 B(x)V(x) \\ \qquad 1 & = A(x)V(x) + B(x)U(x) \end{cases}$$

*for some polynomials $A(x)$, $B(x)$, $U(x)$, $V(x)$ in $K[x]$.*

**Proof.** Due to Lemma 1, $f \circ g$ is reducible over $K$ if and only if $g(x) - \alpha = g(x) - \frac{b}{2a} - \sqrt{\Delta_0}$ is reducible over $K(\sqrt{\Delta_0})$. That is, we may write

$$g(x) - \frac{b}{2a} - \sqrt{\Delta_0} = (A(x) - \sqrt{\Delta_0}\ B(x))(U(x) - \sqrt{\Delta_0}\ V(x))$$

for some polynomials $A(x)$, $B(x)$, $U(x)$, $V(x)$ in $K[x]$. This is equivalent to

$$g(x) - \frac{b}{2a} = A(x)U(x) + \Delta_0 B(x)V(x) \text{ and } 1 = A(x)V(x) + B(x)U(x). \square$$

**Theorem 4.** *Let $f(x) = ax^2 - bx + c \in K[x]$ be an irreducible polynomial. Then there are infinitely many $g(x) \in K[x]$ such that $f \circ g$ is reducible over $K[x]$.*

**Proof.** Let $A(x)$ and $B(x)$ in $K[x]$ be any two relatively prime polynomials. Then $A(x)V(x) + B(x)U(x) = 1$ for $U(x)$, $V(x) \in K[x]$.

For $\Delta = b^2 - 4ac$ and $\Delta_0 = \frac{\Delta}{4a^2}$, define a polynomial $g_0(x) \in K[x]$ by

$$g_0(x) = A(x)U(x) + \Delta_0 B(x)V(x) + \frac{b}{2a},$$

and for any $\lambda(x) \in K[x]$ we let

$$g(x) = g_0(x) + \lambda(x)\left(A(x)^2 - \Delta_0 B(x)^2\right).$$

Then with a root $\alpha = \frac{b}{2a} + \sqrt{\Delta_0}$ of $f(x)$, we have

$$\begin{aligned} & g_0(x) - \alpha = g_0(x) - \frac{b}{2a} - \sqrt{\Delta_0} \\ = \ & A(x)U(x) + \Delta_0 B(x)V(x) - \sqrt{\Delta_0}(A(x)V(x) + B(x)U(x)) \\ = \ & (A(x) - \sqrt{\Delta_0}B(x))(U(x) - \sqrt{\Delta_0}V(x)) \end{aligned}$$

because $A(x)V(x) + B(x)U(x) = 1$. And we also have

$$\begin{aligned} & g(x) - \alpha = g_0(x) + \lambda(x)(A(x)^2 - \Delta_0 B(x)^2) - \alpha \\ = \ & g_0(x) - \alpha + \lambda(x)(A(x) + \sqrt{\Delta_0}B(x))(A(x) - \sqrt{\Delta_0}B(x)) \\ = \ & (A(x) - \sqrt{\Delta_0}B(x))(U(x) - \sqrt{\Delta_0}V(x)) \\ & \quad + \lambda(x)(A(x) + \sqrt{\Delta_0}B(x))(A(x) - \sqrt{\Delta_0}B(x)) \\ = \ & (A(x) - \sqrt{\Delta_0}B(x))[(U(x) + \lambda(x)A(x)) - \sqrt{\Delta_0}(V(x) - \lambda(x)B(x))] \end{aligned}$$

This shows that $g_0(x) - \alpha$ and $g(x) - \alpha$ are reducible over $K(\alpha)$, thus due to Capelli, both $f \circ g_0$ and $f \circ g$ are reducible in $K$ with infinitely many polynomials $\lambda(x)$. $\square$

Refer to [1] for Theorem 4. We shall construct examples of irreducible polynomials $f$ and $g$ such that their composition $f \circ g$ is reducible.

Example 3. Let $f(x) = x^2 - x + 1$. Then $\Delta_0 = -\frac{3}{4}$, $\alpha = \frac{1}{2}(1 + i\sqrt{3})$, so $f(x)$ is irreducible over $\mathbb{Q}$. Let $A(x) = x^2 + 1$ and $B(x) = x - 1$. Then it is easy to see that $\gcd(A(x), B(x)) = 1$ and

$$A(x)V(x) + B(x)U(x) = 1 \text{ with } V(x) = \frac{1}{2},\ U(x) = -\frac{1}{2}(x+1).$$

Let

$$g_0(x) = A(x)U(x) + \Delta_0 B(x)V(x) + \frac{b}{2}$$

Then

$$g_0(x) = \frac{1}{2}(-x^3 - x^2 - \frac{7}{4}x + \frac{3}{4})$$

is irreducible while

$$\begin{aligned} g_0(x) - \alpha &= -\frac{1}{8}(2x^2 + 2 + i\sqrt{3}(-x+1))(2x + 2 + i\sqrt{3}) \\ &= (A - \sqrt{\Delta_0}B)(U - \sqrt{\Delta_0}V) \end{aligned}$$

is reducible. Now take any polynomial $\lambda(x)$, for instance, $\lambda(x) = x + 2$. Let

$$g(x) = g_0(x) + \lambda(x)\left(A(x)^2 - \Delta_0 B(x)^2\right).$$

Then

$$g(x) = x^5 + 2x^4 + \frac{9}{4}x^3 + \frac{7}{2}x^2 - \frac{17}{8}x + \frac{31}{8}$$

is irreducible, while

$$\begin{aligned} g(x) - \alpha &= \tfrac{1}{8}(2x^2+2+i\sqrt{3}(-x+1))(4x^3+8x^2+2x+6+i\sqrt{3}(2x^2+2x-5)) \\ &= (A - \sqrt{\Delta_0}B)[(U - \sqrt{\Delta_0}V) + \lambda(A + \sqrt{\Delta_0}B)] \end{aligned}$$

is reducible. Hence, the reducibility of $g - \alpha$ implies $f \circ g$ is reducible.

Example 4. With the same irreducible polynomial $f(x) = x^2 - x + 1$ as in Example 3, we choose a different set of relatively prime polynomials $A(x) = x^2 + x + 1$ and $B(x) = x - 2$. Clearly $\gcd(A(x), B(x)) = 1$ and

$$A(x)V(x) + B(x)U(x) = 1 \text{ with } V(x) = \frac{1}{7},\ U(x) = -\frac{1}{7}(x+3).$$

Since $\Delta_0 = -\frac{3}{4}$ and $\alpha = \frac{1}{2}(1 + i\sqrt{3})$,

$$g_0(x) = A(x)U(x) + \Delta_0 B(x)V(x) + \frac{b}{2} = \frac{1}{2}(-x^3 - 4x^2 - \frac{19}{4}x + 2)$$

is irreducible while

$$g_0(x) - \alpha = -\frac{1}{28}(2x^2 + 2x + 2 + i\sqrt{3}(-x+2))(2x + 6 + i\sqrt{3})$$

is reducible. Take any polynomial $\lambda(x)$, for instance, $\lambda(x) = x^2 + 2$. Then

$$g(x) = x^6 + 2x^5 + \frac{23}{4}x^4 + \frac{20}{7}x^3 + \frac{153}{14}x^2 - \frac{75}{28}x + \frac{58}{7}$$

while

$$g(x) - \alpha = \tfrac{1}{28}(2x^2 + 2x + i\sqrt{3}(-x + 2)) \cdot (14x^4 + 14x^3 + 42x^2 + 26x + 22 + i\sqrt{3}(7x^3 - 14x^2 + 14x - 29))$$

is reducible. Hence $f \circ g$ is reducible.

We consider another example that involves different polynomials for $h(x)$.

Example 5. Let $f(x) = x^2 - 2x + 3$. Then $f(x)$ is irreducible over $\mathbb{Q}$ with $\Delta_0 = -2$ and root $\alpha = 1 + i\sqrt{2}$. Let $A(x) = x^2 + x + 1$ and $B(x) = x^2 + 1$. Then $\gcd(A(x), B(x)) = 1$ and

$$A(x)V(x) + B(x)U(x) = 1 \text{ with } \ V(x) = -x,\ U(x) = 1 + x.$$

Thus

$$g_0(x) = A(x)U(x) + \Delta_0 B(x)V(x) + \frac{b}{2} = 3x^3 + 2x^2 + 4x + 2$$

while

$$g_0(x) - \alpha = \frac{1}{3}(3x^2 + x + 3 + i\sqrt{2}x)(3x + 1 - i\sqrt{2})$$

reducible. Now take any $\lambda(x)$, for example a cubic $\lambda(x) = x^3 + 1$. Then

$$g(x) = 3x^7 + 2x^6 + 7x^5 + 5x^4 + 8x^3 + 9x^2 + 6x + 5$$

while

$$g(x) - \alpha = \tfrac{1}{3}(3x^2 + x + 3 + i\sqrt{2}x) \cdot (3x^5 + x^4 + 3x^3 + 3x^2 + 4x + 4 + i\sqrt{2}(-x^4 - x - 1))$$

reducible. Hence $f \circ g$ is reducible.

This shows that, for a given irreducible quadratic polynomial $f(x)$, it can be constructed infinitely many polynomials $g(x)$ that makes $f \circ g$ is reducible, by taking any two relatively prime polynomials. The next theorem provides more explicit criteria for the irreducibility of composition polynomials when $g(x)$ is quadratic.

**Theorem 5.** *Let $f(x) = x^2 - bx + c$ irreducible and $g(x) = x^2 + Ax + B$ be*

$$A = t_0\sqrt{-\frac{t}{s_0}} + s\sqrt{-\frac{s_0}{t}}, \quad B = st_0 + ts_0\Delta_0 + \frac{b}{2} \quad (s, t, s_0, t_0 \in \mathbb{Z})$$

*with* $\gcd(s, t) = 1$ *and* $ss_0 + tt_0 = 1$. *If* $-\frac{t}{s_0} \in \mathbb{Q}^2$ *then* $f \circ g$ *is reducible over* $\mathbb{Q}$.

**Proof.** Let $\alpha = \frac{b}{2} + \sqrt{\Delta_0}$ with $\Delta_0 = \frac{b^2-4c}{4}$. Since $f(x)$ is irreducible, $f \circ g$ is reducible if and only if $g(x) - \alpha = g(x) - \frac{b}{2} - \sqrt{\Delta_0}$ is reducible over $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\Delta_0})$ by Lemma 1. Since $g(x)$ is of degree 2, we may factorize $g(x) - \alpha$ as

$$\begin{aligned} & g(x) - \frac{b}{2} - \sqrt{\Delta_0} = \left((rx+s) - t\sqrt{\Delta_0}\right)\left((ux+v) - w\sqrt{\Delta_0}\right) \\ = \;& rux^2 + (vr+su)x + (sv + tw\Delta_0) - \sqrt{\Delta_0}\left((rw+tu)x + (sw+tv)\right) \end{aligned}$$

for some $r, s, t, u, v, w \in \mathbb{Q}$, $(r, u \neq 0)$. Thus we have

$$g(x) - \frac{b}{2} = rux^2 + (vr+su)x + (sv + tw\Delta_0)$$

and $rw+tu = 0$ and $sw+tv = 1$. Without loss of generality we assume $g(x)$ is monic, so $u = \frac{1}{r}$ with $r \neq 0$. Hence from $rw + tu = 0$, we have $r^2w + t = 0$, i.e., $r = \sqrt{-\frac{t}{w}}$ with $-\frac{t}{w} \in \mathbb{Q}^2$. Moreover since $sw + tv = 1$ we may consider $\gcd(s,t) = 1$ for $s, t, v, w \in \mathbb{Z}$.

Now let $g(x) = x^2 + Ax + B$ such that

$$A = t_0\sqrt{-\frac{t}{s_0}} + s\sqrt{-\frac{s_0}{t}}, \quad B = st_0 + ts_0\Delta_0 + \frac{b}{2}$$

such that $\gcd(s,t) = 1$ with $ss_0 + tt_0 = 1$ for $s_0, t_0 \in \mathbb{Z}$. Then $g(x) \in \mathbb{Q}[x]$. If we set $r = \sqrt{-\frac{t}{s_0}} \in \mathbb{Q}$ then $0 = s_0r^2 + t$ so

$$0 = s_0r + \frac{t}{r} = s_0\sqrt{-\frac{t}{s_0}} + t\sqrt{-\frac{s_0}{t}}.$$

Hence with $ss_0 + tt_0 = 1$ we have

$$\begin{aligned} & \left(\sqrt{-\frac{t}{s_0}}x + s - t\sqrt{\Delta_0}\right)\left(\sqrt{-\frac{s_0}{t}}x + t_0 - s_0\sqrt{\Delta_0}\right) \\ = \;& x^2 + \left(s\sqrt{-\frac{s_0}{t}} + t_0\sqrt{-\frac{t}{s_0}}\right)x + st_0 + s_0t\Delta_0 \\ & -\sqrt{\Delta_0}\left(-\left(s_0\sqrt{-\frac{t}{s_0}} + t\sqrt{-\frac{s_0}{t}}\right)x + ss_0 + tt_0\right) \\ = \;& x^2 + \left(t_0\sqrt{-\frac{t}{s_0}} + s\sqrt{-\frac{s_0}{t}}\right)x + (st_0 + ts_0\Delta_0) + \frac{b}{2} - \frac{b}{2} - \sqrt{\Delta_0} \\ = \;& g(x) - \frac{b}{2} - \sqrt{\Delta_0} = g(x) - \alpha. \end{aligned}$$

Thus $g(x) - \alpha$ is reducible over $\mathbb{Q}(\alpha)$, so $f \circ g$ is reducible over $\mathbb{Q}$. □

Example 6. Choose any $s, t$ such that $\gcd(s,t) = 1$ satisfying $ss_0 + tt_0 = 1$ and $-\frac{t}{s_0} = r^2 \in \mathbb{Q}^2$.

| $f(x)$ | $s$ | $t$ | $s_0$ | $t_0$ | $r = \sqrt{-\frac{t}{s_0}}$ | $\Delta$ | $\Delta_0$ | $\alpha$ |
|---|---|---|---|---|---|---|---|---|
| (1) $x^2 - x + 1$ | 3 | 4 | $-1$ | 1 | 2 | $-3$ | $-\frac{3}{4}$ | $\frac{1}{2} + \sqrt{-\frac{3}{4}}$ |
| (2) $x^2 - x + 1$ | 15 | 16 | $-1$ | 1 | 4 | $-3$ | $-\frac{3}{4}$ | $\frac{1}{2} + \sqrt{-\frac{3}{4}}$ |
| (3) $x^2 - 2x - 1$ | 3 | 4 | $-1$ | 1 | 2 | 8 | 2 | $1 + \sqrt{2}$ |
| (4) $x^2 - 2x - 1$ | 8 | 9 | $-1$ | 1 | 3 | 8 | 2 | $1 + \sqrt{2}$ |
| $\cdots$ | | | | | | | | |

In the first two cases we have the same polynomial $f(x) = x^2 - x + 1$ which is irreducible. In (1), let $s = 3$ and $t = 4$. Then

$$g(x) = x^2 + (rt_0 + \frac{s}{r})x + (st_0 + ts_0\Delta_0) + \frac{b}{2} = x^2 + \frac{7}{2}x + \frac{13}{2}$$

is irreducible. And of course

$$g(x) - \alpha = ((2x+3) - 4\sqrt{-\frac{3}{4}})((\frac{1}{2}x + 1) + \sqrt{-\frac{3}{4}})$$

is reducible. Moreover
$f \circ g(x) = x^4 + 7x^3 + \frac{97}{4}x^2 + 42x + \frac{147}{4} = \frac{1}{4}(4x^2 + 12x + 21)(x^2 + 4x + 7)$ is reducible. In (2), with the same $f(x)$ choose $s = 15$ and $t = 16$. Then

$$g(x) = x^2 + \frac{31}{4}x + \frac{55}{2}$$

is irreducible but

$$f \circ g(x) = \frac{1}{16}(16x^2 + 120x + 417)(x^2 + 8x + 28)$$

is reducible. In cases (3) and (4), we take another irreducible polynomial $f(x) = x^2 - 2x - 1$ with $\Delta_0 = 2$ and $\alpha = 1 + \sqrt{2}$. When $s = 3$ and $t = 4$, we have

$$g(x) = x^2 + \frac{7}{2}x - 4$$

is irreducible while $g(x) - \alpha = ((2x+3) - 4\sqrt{2})((\frac{1}{2}x + 1) + \sqrt{2})$ and

$$f \circ g(x) = \frac{1}{4}(4x^2 + 12x - 23)(x^2 + 4x - 4)$$

are reducible. On the other hand, by choosing $s = 8$ and $t = 9$, we have

$$g(x) = x^2 + \frac{17}{3}x - 9$$

is irreducible while $f \circ g(x) = \frac{1}{9}(x^2+6x-9)(9x^2+48x-98)$ is reducible. It concludes that, for a given irreducible polynomial $f(x)$ we can construct infinitely many $g(x)$ explicitly such that $f \circ g$ is reducible.

## 4. The $t$-th iterate of polynomials

The irreducibility of 2nd iterate is based on the Capelli theorem.

**Lemma 6.** [4] *$g \circ f$ is irreducible in $K[x]$ if and only if $g(x)$ is irreducible in $K[x]$ and $f(x) - \beta$ is irreducible in $K(\beta)[x]$ for every root $\beta$ of $g(x)$.*

This can be extended to any $t$-th iterate so that we may be able to construct polynomials explicitly.

**Theorem 7.** *Let $g(x) \in K[x]$ be irreducible. For any $f(x) \in K[x]$, $g \circ f_{t+1}$ is irreducible in $K[x]$ if and only if $f(x) - \beta_t$ and $f(x) - f_j(\beta_t)$ $(0 \le j \le t)$ are irreducible in $K(\beta_t)[x]$ for all roots $\beta_t$ of $g \circ f_t(x)$.*

**Proof.** The case of $t = 0$ is the Lemma 6. When $t = 1$, $g \circ f_2$ is irreducible over $K \Leftrightarrow g \circ f$ is irreducible over $K$ and $f(x) - \beta_1$ is irreducible over $K(\beta_1)$ for every root $\beta_1$ of $g \circ f(x) \Leftrightarrow f(x) - \beta$ is irreducible over $K(\beta)$ and $f(x) - \beta_1$ is irreducible over $K(\beta_1)$ for every roots $\beta$ of $g(x)$ and $\beta_1$ of $g \circ f(x)$.

For every root $\beta_1$ of $g \circ f$, $f(\beta_1)$ is a zero of $g(x)$. Hence if we let $\beta = f(\beta_1)$, then $g \circ f_2$ is irreducible if and only if $f(x) - f(\beta_1)$ is irreducible over $K(f(\beta_1))$ and $f(x) - \beta_1$ is irreducible over $K(\beta_1)$ for every root $\beta_1$ of $g \circ f(x)$. But since $K(f(\beta_1)) = f(K(\beta_1)) = K(\beta_1)$, $g \circ f_2$ is irreducible if and only if both $f(x) - f(\beta_1)$ and $f(x) - \beta_1$ are irreducible over $K(\beta_1)$ for every root $\beta_1$ of $g \circ f(x)$.

Similarly $g \circ f_3$ is irreducible over $K$ if and only if $g \circ f_2$ is irreducible over $K$ and $f(x) - \beta_2$ is irreducible over $K(\beta_2)$ for every root $\beta_2$ of $g \circ f_2(x)$. This is equivalent to that $f(x) - f(\beta_1)$ and $f(x) - \beta_1$ are irreducible over $K(\beta_1)$ and $f(x) - \beta_2$ is irreducible over $K(\beta_2)$ for every roots $\beta_1$ of $g \circ f(x)$ and $\beta_2$ of $g \circ f_2(x)$. But every root $\beta_2$ of $g \circ f_2$ satisfies that $f(\beta_2)$ is a zero of $g \circ f(x)$. Hence if we let $\beta_1 = f(\beta_2)$ then $g \circ f_3$ if irreducible if and only if $f(x) - f_2(\beta_2)$ and $f(x) - f(\beta_2)$ are irreducible over $K(f(\beta_2))$ and $f(x) - \beta_2$ is irreducible over $K(\beta_2)$ for every root $\beta_2$ of $g \circ f_2(x)$, hence it is so if and only if $f(x) - f_2(\beta_2)$, $f(x) - f(\beta_2)$ and $f(x) - \beta_2$ are irreducible over $K(\beta_2)$ for every root $\beta_2$ of $g \circ f_2(x)$.

Therefore $g \circ f_{t+1}$ is irreducible over $K$ if and only if $f(x) - f_j(\beta_t)$ $(1 \le j \le t)$ and $f(x) - \beta_t$ are irreducible over $K(\beta_t)$ for every root $\beta_t$ of $g \circ f_t(x)$. $\square$

**Acknowledge.** I would like to thank the referee for the valuable comments.

## References

[1] N. Ali, On the irreducibility for composition of polynomials. International Mathematical Forum, 4, (40), 2009, 2001-2008

[2] L. Danielson, B. Fein. On the irreducibility of iterates of $x^n - b$, The Americal Math. Soc. 130 (2011), 1589-1596.

[3] R.K.W. Odoni. The Galois theory of iterates and composites of polynomials, Prod. London Math Soc. (3), 51 (3), 1985, 385-414

[4] R.K.W. Odoni. On the prime divisors of the sequence $w_{n+1} = 1 + w_1 \cdots w_n$. J. London Math. Soc. 32 (1985), 1-11.

Eunmi Choi
Department of Mathematics, HanNam University,
Daejon 306-791, Korea.
E-mail: emc@hnu.kr