On the Irreducibility for
Composition of Polynomials

Nidal Ali

Université du Littoral Côte d’Opale
50 rue F. Buisson, F-62228 Calais Cedex, France
nidal@lmpa.univ-littoral.fr
Ali.Nidal@lmpa.univ-littoral.fr

Abstract

Given an Hilbertian field $K$, a polynomial $g(x) \in K[x]$ and an integer $n \in \mathbb{N}$, we show that there exist infinitely many polynomials $f(x) \in K[x]$ of degree $n$ such that $f \circ g(x)$ is irreducible over $K$. On the other hand, if $f(x) = x^2 - d \in K[x]$ be an irreducible polynomial, then we show that there exist infinitely many polynomials $g(x) \in K[x]$ non strictly composite such that $f \circ g(x)$ is reducible over $K$.

Mathematics Subject Classifications: 11C, 12Y08

Keywords: Composition of polynomials, Irreducibility, Hilbertian fields

1 Introduction

Let $f(x)$ and $g(x)$ are two polynomials in $K[x]$, under what conditions the polynomial $f \circ g(x)$ is irreducible? We will state some results about the irreducibility for composition of polynomials. Indeed, Shure in [3] has stated his conjecture defined as follows: If $g(x)$ is a monic polynomial of degree $m$ with distinct integer roots, and $f(x) = x^2^n + 1$. Then $f \circ g(x)$ is irreducible over $\mathbb{Q}$ except for $n = 0, m \leq 4$. This conjecture was proved for $n = 0$ by Flügel in [7], for $n = 1$ in the book of G. Pólya and G. Szegő [9], for $n = 2$ by H. Ille in [8] and for $n \leq 3$ in a more general form by A Brauer, R. Brauer and H. Hopf in [4].

In [1], The authors have obtained the irreducibility of all iterates of a quadratic polynomial over a field, in term of its discriminant. Some related results to the irreducibility of $f \circ g(x)$ for certain polynomials $f(x)$ of the second and fourth degree and for $g(x)$ having distinct roots in an imaginary quadratic field have been obtained by H.L. Dorwat and O. Ore (See [6]).
Let $K$ be a field, the polynomial $f(x) \in K[x]$ is said to be strictly composite if there exist two polynomials over $K$, $u(x)$, $g(x)$ both of them of degrees at least two such that $f(x) = u(g(x))$.

**Definition 2** Let $K$ be a field, $K$ is said to be hilbertian, if for every irreducible polynomial $P(X_1, ..., X_r, Y_1, ..., Y_s)$ in $K[X_1, ..., X_r, Y_1, ..., Y_s]$ (with $r, s \geq 1$), there exist infinitely many $(x_1^*, ..., x_r^*) \in K^r$ such that $P(x_1^*, ..., x_r^*, Y_1, ..., Y_s)$ is irreducible in $K[Y_1, ..., Y_s]$.

For example, an algebraic number field is hilbertian field.

**Theorem 1** Let $K$ be an hilbertian, $f(x) = x^2 - d \in K[x]$, be irreducible polynomial over $K$, then there exist infinitely many polynomials $g(x) \in K[x]$ non strictly composite such that $f \circ g(x)$ is reducible over $K$.

Now, we fix a polynomial $g(x) \in K[x]$, then we will study the set of polynomials $f(x) \in K[x]$ so that $f \circ g(x)$ is irreducible over $K$.

**Theorem 2** Let $K$ be a field, $f(x) \in K[x]$, be an irreducible polynomial over $K$ and $g(x) \in K[x]$. Then the following two conditions are equivalent:
i) The polynomial $f \circ g(x)$ is reducible over $K$.
ii) The ideal $\langle f(x) \rangle$ is not prime in the ring $A = K[x, \xi]$, where $\xi$ is a root in $K(x)$ of the polynomial $g(y) - x$.

**Theorem 3** Let $K$ be an hilbertian field, $g(x) \in K[x]$ be a polynomial and $n \geq 1$ an integer, then there exist infinitely many polynomials $f(x) \in K[x]$ such that $\deg f = n$ and $f \circ g(x)$ is irreducible over $K$. 
2 Preliminaries lemmas

To show our results we need to the following lemmas.

**Lemma 1 (Capelli’s lemma 1)** Let $K$ be a field, $f(x)$, $g(x)$ are two polynomials in $K[x]$ and let $\alpha$ be a root of $f(x)$ in an algebraic closure of $K$, then the following two conditions are equivalent:

i) $f \circ g(x)$ is irreducible over $K$.

ii) $f(x)$ is irreducible over $K$ and $g(x) - \alpha$ is irreducible over $K(\alpha)$.

**Proof.** See ([14], Satz 4, p.288).

**Lemma 2** Let $K$ be a field, $f(x) = x^2 - d \in K[x]$, an irreducible polynomial over $K$ and $g(x) \in K[x]$ a polynomial, then:

The polynomial $f \circ g(x)$ is reducible over $K$, if and only if, there exist $A(x), B(x), U(x), V(x)$, in $K[x]$, $A(x)$ is prime with $B(x)$, $A(x).B(x) \notin K, U(x).V(x) \notin K$ such that:

$$\begin{cases}
A(x).U(x) + B(x).V(x) = 1 \\
A(x).V(x) + dB(x).U(x) = g(x).
\end{cases}$$

**Proof.** Using lemma 1, the polynomial $f \circ g(x)$ is reducible over $K \iff g(x) + \sqrt{d}$ is reducible over $K(\sqrt{d}) \iff \exists A(x), B(x), U(x), V(x) \in K[x]$ with $A(x)$ or $B(x)$, $U(x)$ or $V(x)$ are not in $K$, such that: $g(x) + \sqrt{d} = [A(x) + \sqrt{d}.B(x)].[V(x) + \sqrt{d}.U(x)] \iff$

$$\begin{cases}
A(x).U(x) + B(x).V(x) = 1 \\
A(x).V(x) + dB(x).U(x) = g(x)
\end{cases}$$

**Lemma 3** Let $K$ be a field, $f(x) = x^2 - d \in K[x]$, an irreducible polynomial over $K$, and $A(x), B(x) \in K[x]$ are relatively prime polynomials such that $A$ or $B$ is not constant. We denote by: $U_0(x), V_0(x)$ the unique polynomials that verify:

$A(x).U_0(x) + B(x).V_0(x) = 1$ with $\deg U_0 < \deg B$ and $\deg V_0 < \deg A$. Let :

$g_0(x) = A(x).V_0(x) + dB(x).U_0(x)$. So, for every $\lambda(x) \in K[x]$, the polynomial

$g_\lambda(x) = g_0(x) + \lambda(x)[A(x)^2 - dB(x)^2]$ verifies that $f \circ g_\lambda(x)$ is reducible over $K$.

**Proof.** For every $\lambda(x) \in K[x]$, consider the polynomial

$$g_\lambda(x) + \sqrt{d} = g_0(x) + \sqrt{d} + \lambda(x)[A(x)^2 - dB(x)^2].$$
By Lemma 2, the polynomial \( f \circ g_0(x) \) is reducible over \( K \) and \( g_0(x) + \sqrt{d} = [A(x) + \sqrt{d}.B(x)].[V_0(x) + \sqrt{d}.U_0(x)] \), hence, we deduce that:

\[
g_\lambda(x) + \sqrt{d} = [A(x) + \sqrt{d}B(x)][\{V_0(x) + \lambda(x)A(x)\} + \sqrt{d}\{U_0(x) - \lambda(x)B(x)\}].
\]

The polynomials \( V_0(x) + \lambda(x)A(x) \), \( U_0(x) - \lambda(x)B(x) \) are not constant, otherwise, \( \deg V_0 \geq \deg A \) and \( \deg U_0 \geq \deg B \), this implies that the polynomial \( g_\lambda(x) + \sqrt{d} \) is reducible over \( K(\sqrt{d}) \). Finally, the required result follows from lemma 1 and then the polynomial \( f \circ g_\lambda(x) \) is reducible over \( K \).

Lemma 4 Let \( K \) be an hilbertian field, \( g_0(x), p(x) \) are two polynomials in \( K[x] \) of degree \( k, n \) respectively such that \( k < n \), then, for every \( l > n \), there exist infinitely many polynomials \( g(x) \) of degree \( l \) such that:

\[
g(x) \equiv g_0(x) \mod p(x) \text{ and } g(x) \text{ is not strictly composite.}
\]

Proof. First, Note that if \( f \) is strictly composite then \( f' \) is reducible over \( K \). Let \( m \geq 1 \) be an integer such that \( l = m + n \). Consider the polynomial:

\[
l(x) = x^m + \ldots + \lambda_1 x + \lambda_0 \text{ where } \lambda_0, \ldots, \lambda_{m-1} \text{ are algebraically independant variables over } K. \text{ Let:}
\]

\[
g_\lambda(x) = g_0(x) + \lambda(x)p(x).
\]

The polynomial \( g'_\lambda(x) \) (derivative of \( g_\lambda(x) \) with respect to \( x \)) is irreducible in \( K[\lambda_0, \ldots, \lambda_{m-1}, x] \). The field \( K \) is hilbertian, so there exist infinitely \( \lambda_0^*, \ldots, \lambda_{m-1}^* \) in \( K \) such that the substituted polynomial:

\[
g'_\lambda^*(x) = g'_\lambda(\lambda_0^*, \ldots, \lambda_{m-1}^*)
\]

is irreducible over \( K \), hence \( g_\lambda^*(x) \) is not strictly composite.

Lemma 5 (Capelli’s lemma 2) Let \( K \) be a field and \( x^n - c \in K[x] \). Then, \( x^n - c \) is reducible over \( K \) if and only if

\[
\begin{cases}
\exists p|n/ : c \in K^p \\
\text{Or} \\
\text{If } 4|n, c \in -4K^4.
\end{cases}
\]

Proof. See [10].
3 Proof of the results

**Proof of theorem 1.** Let $A(x), B(x) \in K[x]$ be two relatively prime polynomials, we know, by lemme 3 that, for every $\lambda(x) \in K[x]$, the polynomial

$$g_\lambda(x) = g_0(x) + \lambda(x)[A(x)^2 - dB(x)^2]$$

verifies that $f \circ g_\lambda(x)$ is reducible over $K$ and for every $l \geq n = \deg[A(x)^2 - dB(x)^2]$, there exist infinitely polynomials $\lambda(x)$ of degree $l - n$ such that $g_\lambda(x)$ is not strictly composite. Thus, we obtain infinitely many polynomials $\lambda(x) \in K[x]$ such that $g_\lambda(x)$ is not strictly composite and $f \circ g_\lambda(x)$ is reducible over $K$.

**Remark** If $f(x) = x^2 - d \in K[x]$, is irreducible polynomial over an Hilbertian field $K$, then we can also find infinitely many polynomials $g(x) \in K[x]$ such that $f \circ g(x)$ is irreducible over $K$. Indeed, let $g(T, x) = T x^n$, then $f \circ g(T, x) = T^2 x^{2n} - d$ is irreducible in $K[T, x]$ by lemma 5. The field $K$ is Hilbertian, so we can find infinitely many $t \in K^*$ such that $f \circ g(t, x)$ is irreducible in $K[x]$. Therefore, the required result follows.

**Proof of theorem 2.** $i \Rightarrow ii)$ Suppose that $f \circ g(x)$ is reducible over $K$, then there exist two polynomials $h_1(x), h_2(x)$ in $K[x]$ of degrees $\geq 1$, such that $f \circ g(x) = h_1(x).h_2(x)$, this implies that $f \circ g(\xi) = h_1(\xi).h_2(\xi)$. But $g(\xi) = x$, so

$$f(x) = h_1(\xi).h_2(\xi).$$

(1)

Suppose that $h_1(\xi)$ or $h_2(\xi)$ is invertible in $A$. Let $h_1(\xi) \in A^*$, $\xi_1 = \xi, \xi_2, ..., \xi_n$ the conjugates of $\xi$ in $K(x)$. They are different from each other because the polynomial $g(y) - x$ is separable in $K[x, y]$. The equation (1) gives,

$$f(x)^n = \prod_{i=1}^{n} h_1(\xi_i). \prod_{i=1}^{n} h_2(\xi_i).$$

Let $a = \prod_{i=1}^{n} h_1(\xi_i)$. Hence $a \in K[x]$, in fact, $a = N_{K(x, \xi)/K(\xi)}(h_1(\xi))$. Thus, $a \in A^* \cap K[x] = K[x]^* = K^*$. We deduce that $f(x)^n = a \prod_{i=1}^{n} h_2(\xi_i) = b.\text{Res}_y(g(y) - x, h_2(y))$, for some $b \in K^*$. Let $\deg h_2 = t, H(x) = \text{Res}_y(g(y) - x, h_2(y))$.

Since $\deg H = \deg h_2 = t$ and $f(x)^n = b.H(x)$, so:

$\deg f \circ g = n. \deg f = t < \deg f \circ g$, which is not possible. Therefore, $f(x)$ is
By substituting \( \Phi(x) = x \) is hilbertian, then, there exist infinitely many elements \( M \). Hence, using Hilbert’s theorem, we can find infinitely many \( g \) such that \( \Phi(g) = x \). Since \( \Phi(g) = x \) is absolutely irreducible (i.e. irreducible over \( K \)), it is irreducible in \( M \). Consequently, \( g(x) = y \) is reducible in \( K \). Using lemma 1, we deduce that \( f \circ g(x) \) is reducible over \( K \).

**Proof of theorem 3.** Let \( M/K \) be an extension of degree \( n \). The field \( M \) exists. Indeed, \( K \) is hilbertian, then there exists at least one irreducible polynomial of degree \( n \), obtained by substituting in \( K^n \) the polynomial \( F(s_1, ..., s_n, x) = x^n - s_1x^{n-1} + ... + (-1)^ns_n \). The field \( K \) is hilbertian then \( M \) is so (See [10], Theorem 48). Consider the polynomial,

\[
G(x, y) = g(x) - y.
\]

It is absolutely irreducible (i.e. irreducible over \( K \)) so irreducible in \( M[x, y] \). Hence, using Hilbert’s theorem, we can find infinitely many \( l \in M \) such that the polynomial \( g(x) - l \) is irreducible in \( M[x] \). The elements \( l \) can be taken as primitive elements of \( M \). Indeed, Let \( \{w_1, ..., w_n\} \), be a basis of \( M/K \), \( u_1, ..., u_n \) are \( n \) algebraically independent variables over \( K \), \( \xi = u_1.w_1 + ... + u_n.w_n \) and

\[
F(u_1, ..., u_n, x) = \prod_{i=1}^{n} (x - \xi_{\sigma_i}) = \text{Irr}[\xi, K(u_1, ..., u_n), x]
\]

be the generic polynomial of the field \( M \) over \( K \) where \( \sigma_1, ..., \sigma_n \) are \( n \)-distinct canonical imbedding of \( M \) in \( K \) and \( \xi_{\sigma_i} = u_1.\sigma_i(w_1) + ... + u_n.\sigma_i(w_n) \). By substituting \( u_1, ..., u_n \) in \( K^n \), we get the characteristic polynomial

\[
F(u_1^*, ..., u_n^*, x) = [\text{Irr}(\xi^*, K, x)]^d
\]

where \( \xi^* = u_1^*.w_1 + ... + u_n^*.w_n \), \( d = n/t \) and \( t = [K(\xi^*): K] \).

Consider now the discriminant with respect to \( x \) of \( F(u_1, ..., u_n, x) \) denoted by \( \Phi(u_1, ..., u_n) \) and let

\[
V_\Phi = \{(u_1^*, ..., u_n^*) \in K^n \text{ tel que } \Phi(u_1^*, ..., u_n^*) = 0\}
\]

This is an algebraic manifold considered as a Zariski’s closed of \( K^n \). Again, \( M \) is hilbertian, then, there exist infinitely elements \( l = u_1^*.w_1 + ... + u_n^*.w_n \in M \) such that \( \Phi(u_1^*, ..., u_n^*) \neq 0 \) (outside \( V_\Phi \)) and \( G(x, l) \) is irreducible in \( M[x] \). Since \( \Phi(u_1^*, ..., u_n^*) = \text{disc}_x F(u_1^*, ..., u_n^*, x) \neq 0 \), we deduce that \( F(u_1^*, ..., u_n^*, x) \) is separable in \( K[x] \), which implies that \( n = t \), thus, \( [l, K] = n \). Therefore, \( l \) is primitive element of \( M/K \).
Set $f(x) = \text{Irr}(l, K, x)$, hence, $\deg f = n$. Using lemma 1, we deduce that the polynomial $f \circ g(x)$ is irreducible over $K$. □

Note that, if $K$ is an arbitrary field. Then, by ([16], theorem 1), it need not follow that the extension $M/K$ of degree $n$ exists.

References


**Received: March, 2009**