International Journal of Algebra, Vol. 12, 2018, no. 4, 149 - 156
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ija.2018.825

A New Method for Stability of Polynomials

Nidal Ali

Lebanese university, Faculty of Sciences 1
Mathemetics Department, Lebanon

Abstract

Using the calculation of the resulting of polynomials, we describe in this paper a new method to prove the stability of a polynomial $f(x)$ of second degree, that is the irreducibility of all the iterates of f.

Mathematics Subject Classification: 11R09, 11T06, 12E10

Keywords: Polynomials, irreducibility, iteration, stability, hilbertian field

1 Introduction

Let K be a field, $f(x) \in K[x]$. Set $f_1(x) = f(x)$ and for every $m \geq 2$, $f_m(x) = (f_{m-1} \circ f)(x)$. We say that f is a *stable polynomial* over K if for all $m \geq 1$, $f_m(x)$ is irreducible over K.

For example, given a prime number p. A polynomial $f(x) = a_n x^n + \ldots + a_1 x + a_0$ in $\mathbb{Z}[x]$ is said to be p^r-eisenstein for some $r \wedge n = 1$ if p^r divides $a_0, \ldots, a_{n-1}$, p^{r+1} does not divide a_0 and p does not divide a_n.
In [1], the author proved the stability in $\mathbb{Z}[x]$ of this polynomial.

In [2], [3], [4] the authors have also studied the stability. For example, in [3], they proved the stability in $\mathbb{Z}[x]$ of all irreducible polynomial of the form $x^n - c$.

Definition 1. Let $K = \mathbb{Q}(\theta)$ be a number field of degree n, A'_K is its ring of integers, $\{w_1, \ldots, w_n\}$ is an integral basis of K or simply a basis of A'_K. Let

$u_1, ..., u_n$ are algebraically independent variables over K, $\xi = u_1.w_1 + \ldots + u_n.w_n$. We define the generic polynomial of integers of K to be

$$F(u_1, \ldots, u_n, x) = Irr(\xi, L, x)$$

where $L = \mathbb{Q}(u_1, \ldots, u_n)$.

The polynomial $F(u_1, \ldots, u_n, x)$ is generic because, in substituting $(u_1, \ldots, u_n)$ in $\mathbb{Z}^n$, we get a generic element $\xi^* = u_1^* w_1 + \ldots + u_n^* w_n$ in A'_K and the characteristic polynomial $F(u_1^*, \ldots, u_n^*, x) = [Irr(\xi^*, \mathbb{Q}, x)]^{n/t}$ where $t = [\mathbb{Q}(\xi^*) : \mathbb{Q}]$. Hence, the minimal polynomial of any element of A'_K can be deduced from $F(u_1, \ldots, u_n, x)$.

Definition 2. Given two non zero natural integers n, e and a prime number p in $\mathbb{Z}$. We define the property $S(n, p, e)$ by: There exists a monic irreducible polynomial of degree n stable over $\mathbb{F}_{p^e}$.

In [1], the author proved the following two theorems:

Theorem 1. *Let K be a number field of degree n, A'_K is its ring of integers and let p be a prime number of $\mathbb{Z}$ totally ramified in K then:*
i) There exist infinitely many α of $K \setminus \mathbb{Q}$ such that $K = \mathbb{Q}(\alpha)$ and the minimal polynomial of α is stable sur $\mathbb{Q}$.
ii) The generic polynomial of integers of K, $F(u_1, \ldots, u_n, x)$ is stable in the ring $\mathbb{Z}[u_1, ..., u_n, x]$.

Theorem 2. *Consider an odd prime number p. For any integer $e \geq 1$, the property $S(2, p, e)$ is true. That is, we can always find a monic quadratic polynomial stable over $\mathbb{F}_{p^e}$.*

Note that in theorem 2, the author has built many quadratic stable polynomials over $\mathbb{F}_{p^e}$. This is according to the values of p^e. In fact, the first case $p^e \equiv 1 \pmod 4$ gives a set of such polynomials and the second case $p^e \equiv -1 \pmod 4$ gives also another set of quadratic stable polynomials in $\mathbb{F}_{p^e}[x]$.

2 Main results

In this section, we will state our main result. It is about the stability of a monic irreducible polynomial of second degree. In fact, It is a new algebraic method based on the theory of resulting of polynomials.

Theorem 3. *Let $f(x)$ be a monic irreducible polynomial of second degree in $\mathbb{Z}[x]$. We define the integer C_n to be $C_n := Res_x(f_n(x), f'(x))$ and we suppose, for all $(n, m) \in \mathbb{N}^2$, $n \neq m$ that:*

$$\begin{array}{c} \textit{i) } C_n \wedge C_m = 1. \\ \textit{ii) } \pm C_n \textit{ is not square.} \end{array}$$

Then the polynomial $f(x)$ is stable over $\mathbb{Q}$.

The general form of stability is the irreducibility of the composition of polynomials that will be stated in the following lemma due to Capelli.

Lemma 1 (Capelli)**.** *Let K is field, $f(x)$, $g(x)$ are two polynomials in $K[x]$ and let α be a root of $f(x)$ in an algebraic closure of K. The following statements 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 ([5], Satz 4, p.288).

Notations:
Let $k = \deg f$, then $\deg f_n = k^n$. We denote by:

$$\begin{array}{c} (a_n^i)_{i=1,...,k^n} \text{ to be the roots of } f_n(x). \\ \text{and} \\ (a_{n+1}^j)_{j=1,...,k^{n+1}} \text{ the roots of } f_{n+1}(x). \end{array}$$

Thus, we can write $f_n(x) = \prod_{i=1}^{k^n}(x - a_n^i)$, $f_{n+1}(x) = \prod_{j=1}^{k^{n+1}}(x - a_{n+1}^j)$, which is equal to $f_n(f(x)) = \prod_{i=1}^{k^n}(f(x) - a_n^i)$.

To prove theorem 3, we need to the following lemmas:

Lemma 2. *Let $f(x)$ be a monic irreducible polynomial of degree k in $K[x]$, where K is a field and $n \geq 1$ is an integer such that $f_n(x)$ is irreducible but $f_{n+1}(x)$ is reducible. Set $f_{n+1}(x) = h_1(x)...h_r(x)$. Then, $r \leq k$ and there exists $(d_1, .., d_r) \in \mathbb{N}^r$ such that $\deg h_j = d_j.k^n$ and $1 \leq d_j < k$ for all j.*

Proof.
Let $h_j(x) \in K[x]$ be an irreducible factor of $f_{n+1}(x)$ and let b is a root of $h_j(x)$. Let $f_{n+1}(x) = \prod_{i=1}^{k^n}(f(x) - a_n^i)$. This implies that there exists $i \in \{1, ..., k^n\}$ such that b is a root of $f(x) - a_n^i$. Thus,

$$K \subset K(a_n^i) \subset K(b).$$

We deduce that $k^n \mid \deg h_j$. Let $d_j \in \mathbb{N}^*$ such that $\deg h_j = d_j.k^n$. Since $k^n \leq \deg h_j < k^{n+1}$, it follows that $k^n \leq d_j.k^n < k^{n+1}$. Hence, $1 \leq d_j < k$. Now, $\deg f_{n+1} = k^{n+1} = k^n.\sum_{j=1}^r d_j$ so $\sum_{j=1}^r d_j = k$. Therefore, $r \leq k$. ■

Lemma 3. *Let $f(x)$ be a monic polynomial of degree k in $\mathbb{Z}[x]$. We denote by Δ_n to be the discriminant of $f_n(x)$ and $C_n = Res_x(f_n(x), f'(x))$. We have the following formula:*

$$\Delta_n = \pm C_n \cdot C_{n-1}^k \cdot C_{n-2}^{k^2} \cdot .... \cdot C_1^{k^{n-1}}$$

Proof.
We argue by induction on n. For $n = 1$, it is known that $\Delta_1 = disc(f(x)) = \pm Res_x(f(x), f'(x)) = \pm c_1$. Suppose the formula is true for n so,

$$\Delta_n = \pm C_n \cdot C_{n-1}^k \cdot C_{n-2}^{k^2} \cdot .... \cdot C_1^{k^{n-1}}.$$

We have,

$$\Delta_{n+1} = disc(f_{n+1}(x)) = \pm Res_x(f_{n+1}(x), f'_{n+1}(x)) =$$

$$\pm \prod_{j=1}^{k^{n+1}} f'_{n+1}(a_{n+1}^j) =$$

$$\pm \prod_{j=1}^{k^{n+1}} f'(a_{n+1}^j). \prod_{j=1}^{k^{n+1}} f'_n(f(a_{n+1}^j)) =$$

$$\pm C_{n+1}. \prod_{j=1}^{k^{n+1}} f'_n(f(a_{n+1}^j)).$$

Each factor $f_n(x) - a_n^i$ has k roots of f_{n+1}. We can sort these roots in such a way that:
$(a_{n+1}^j)_{j=1,...,k}$ are the common roots with $f(x) - a_n^1$.
$(a_{n+1}^j)_{j=k+1,...,2k}$, are the common roots with $f(x) - a_n^2$ and then ....
$(a_{n+1}^j)_{j=k^{n+1}-k+1...k^{n+1}}$ with $f(x) - a_n^{k^n}$.
Since a_{n+1}^j is a root of a one of the factors $f(x) - a_n^i$, it follows that $f(a_{n+1}^j) = a_n^i$ is a root of f_n. Thus, we can write:

$$\Delta_{n+1} = \pm C_{n+1}. \prod_{j=1}^{k} . \prod_{i=1}^{k^n} f'_n(a_n^i) = \pm C_{n+1}. \prod_{j=1}^{k} (\Delta_n) = \pm C_{n+1}.(\Delta_n)^k.$$

This implies that

$$\Delta_{n+1} = \pm C_{n+1} \cdot C_n^k \cdot C_{n-1}^{k^2} \cdot .... \cdot C_1^{k^n}.$$

■

Proof of theorem 3.
Suppose that $f(x)$ is not stable in $\mathbb{Z}[x]$. This means that there exists $n \geq 1$

such that $f_n(x)$ is irreducible over $\mathbb{Q}$ but $f_{n+1}(x)$ is reducible. By lemma 2, there exist two irreducible polynomials $g_1(x), g_2(x) \in \mathbb{Z}[x]$ such that

$$f_{n+1}(x) = g_1(x).g_2(x).$$

Consider the following formulas,

$$\Delta_n = \pm C_n \cdot C_{n-1}^2 \cdot C_{n-2}^{2^2} \cdot .... \cdot C_1^{2^{n-1}}, \Delta_{n+1} = \pm C_{n+1} \cdot C_n^2 \cdot C_{n-1}^{2^2} \cdot .... \cdot C_1^{2^n}.$$

Since C_{n+1} is not a square, it follows that there exists a prime number p such that p divides C_{n+1} and the $p-$adic valuation $\vartheta_p(C_{n+1})$ is odd. Note that

$$\vartheta_p(C_{n+1}) = \vartheta_p(\Delta_{n+1}).$$

Indeed, in the formula of Δ_{n+1}, the prime number p can only divides C_{n+1}. For if there exists $t \in \{2, ..., 2^n\}$, $i \in \{1, n\}$ such that $p \mid C_i^t$ then $p \mid C_i$. This implies that $C_i \wedge C_{n+1} \neq 1$, which is not true. Thus, p divides Δ_{n+1} and does not divide Δ_n. Since $f_n(x)$ is irreducible in $\mathbb{Z}[x]$, we can deduce that,

$$\Delta_n = I_n^2.D(K_n)$$

where K_n is one field generated by any root of $f_n(x)$ and $D(K_n)$ is the absolute discriminant of K_n. Now we can deduce that p does not divide $D(K_n)$. This implies that p is not ramified in K_n.
On the other hand, we have:

$$\Delta_{n+1} = disc(f_{n+1}(x)) = disc(g_1(x).g_2(x))$$

$$= disc(g_1(x)).disc(g_2(x)).Res_x(g_1(x), g_2(x))^2$$

$$= I_1^2.D(L_1).I_2^2.D(L_2).Res_x(g_1(x), g_2(x))^2$$

where $disc(g_t(x)) = I_t^2.D(L_t)$ for any $t \in \{1, 2\}$. This implies that there exists $t \in \{1, 2\}$ such that p divides $D(L_t)$, so p is ramified in L_t. Let $L_t = \mathbb{Q}(a_{n+1}^j)$, a_{n+1}^j is a root of g_t. There is $i \in \{1, ..., 2^n\}$ such that a_{n+1}^j is a root of $f(x) - a_n^i$. Thus we have,

$$\mathbb{Q} \subset \mathbb{Q}(a_n^i) \subset \mathbb{Q}(a_{n+1}^j) = L_t.$$

It is clear that both inclusions are strict since $f_n(x)$ is irreducible over $\mathbb{Q}$ and there exists a prime number p ramified in L_t but not in $\mathbb{Q}(a_n^i)$.
Set, $[\mathbb{Q}(a_{n+1}^j) : \mathbb{Q}(a_n^i)] = \gamma$, so $[L_t : \mathbb{Q}] = \deg g_t = \gamma.2^n$. Therefore, we deduce that, $2^n < \gamma.2^n < 2^{n+1}$, which means that $1 < \gamma < 2$. This is impossible since γ is a natural integer. We deduce that $f_n(x)$ is irreducible for all $n \geq 1$. Consequently, the polynomial $f(x)$ is stable over $\mathbb{Q}$. ■

The following statement is assumed to be an open problem. It is in fact about the generic polynomial of a field K.

Definition 3. *A field K is said to be hilbertian, if for every irreducible polynomial $P(X_1, ..., X_r, Y_1, ..., Y_s)$ in $K[X_1, ..., X_r, Y_1, ..., Y_s]$ (where $r, s \geq 1$), there exist an 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 $\mathbb{Q}$ is hilbertian.

Conjecture.
Let K be an hilbertian field. $s_1, ..., s_n$ are n algebraically independent variables. The polynomial $f(x) = x^n + s_1x^{n-1} + \ldots + s_{n-1}x + s_n$ is defined to be the generic polynomial of K. It is stable in $K[s_1, ..., s_n, x]$. Indeed, it is enough to substitute $s_1, ..., s_n$ by one variable Y, and then $f(x)$ will be Y-eisenstein so irreducible. In addition, it is stable over K by [1]. For every $t \geq 1$, let
$I_t = \{(s_1^*, ..., s_n^*) \in K^n$ such that $f_t(s_1^*, ..., s_n^*, x)$ is irreducible over K$\}$. We have

$$... \subseteq I_t \subseteq I_{t-1} \subseteq ... \subseteq I_1.$$

Since K is hilbertian, it follows that I_t is infinite set. Let $I = \bigcap_{t\geq 1} I_t$. Is I infinite? is it non empty set? is there an integer $t(K)$ such that $I_t = I_{t_k}$ for all $t \geq t_k$?

3 Application

Let $f(x) = x^2 - x + 1$, we are going to prove the stability of f over $\mathbb{Q}$. In fact, it is enough to verify the conditions stated in theorem 3. First, let us define the sequence $(C_n)_{n\geq 1}$ by $C_n = Res_x(f_n(x), f'(x)) = 2^{2^n}.f_n(\frac{1}{2})$.
$C_{n+1} = 2^{2^{n+1}}.f_{n+1}(\frac{1}{2}) = 2^{2^{n+1}}.f(f_n(\frac{1}{2}))$. Since $f_n(\frac{1}{2}) = \frac{C_n}{2^{2^n}}$, it follows that C_{n+1} $= 2^{2^{n+1}}.f(\frac{C_n}{2^{2^n}})$. This implies that

$$C_{n+1} = C_n^2 - 2^{2^n}C_n + 2^{2^{n+1}}.$$

Lemma 4. *For all integers n, m such that $1 \leq n < m$, we have:*
i) $C_n > 0$, $C_n \equiv 1 \pmod{2^n}$.
ii) $C_n \wedge C_m = 1$.

Proof.
For every $n \geq 1$, we have,

$$C_{n+1} = C_n^2 - 2^{2^n}C_n + 2^{2^{n+1}} = (C_n - 2^{2^n-1})^2 + 3.2^{2^{n+1}-2}$$

so C_{n+1} is strictly positive. The second statement is clear.
Suppose now there exists a prime number p dividing C_n and C_m then, $C_{n+1} =$

$C_n^2 - 2^{2^n}C_n + 2^{2^{n+1}} \equiv 2^{2^{n+1}} \pmod{p}$.
Since $C_{n+2} = C_{n+1}^2 - 2^{2^{n+1}}C_{n+1} + 2^{2^{n+2}}$, it follows that $C_{n+2} \equiv 2^{2^{n+2}} \pmod{p}$.
Thus we can deduce that

$$C_m \equiv 2^{2^m} \pmod{p}.$$

Now, $p \mid C_m$, so $p \mid 2^{2^m}$. This implies that $p = 2$, which is not true since C_n is odd integer. ■

Lemma 5. *For every $n \geq 1$, C_n is not square in $\mathbb{Z}$.*

Proof.
For $n = 1, 2, 3$, the integers $C_1 = 3, C_2 = 13$ and $C_3 = 217$ are not squares.
Suppose there exists $n \geq 3$ such that C_{n+1} is square in $\mathbb{Z}$, so there exists $a \in \mathbb{Z}$ such that,

$$C_{n+1} = a^2 = C_n^2 - 2^{2^n}C_n + 2^{2^{n+1}}. \tag{1}$$

This implies that $a^2 - C_n^2 \equiv 0 \pmod{8}$, so $(a - C_n) \equiv 0 \pmod{4}$ or $(a + C_n) \equiv 0 \pmod{4}$.
Replacing a by $-a$. We can suppose that $(a - C_n) \equiv 0 \pmod{4}$. Thus, there exists an odd integer e, $t \geq 2$ such that

$$a = C_n + e.2^t. \tag{2}$$

Substituting a in its value in (1), we get:

$$(e \cdot C_n + e^2 \cdot 2^{t-1})2^{t+1} = 2^{2^n}(-C_n + 2^{2^n}). \tag{3}$$

But $(e.C_n + e^2 \cdot 2^{t-1})$ and $(-C_n + 2^{2^n})$ are odd, so $2^{t+1} = 2^{2^n}$. Hence $t = 2^n - 1$.
Since $n \geq 3$, it follows that $t \geq 7$. Replacing 2^n by $t + 1$ in (3), we get:

$$C_n(e + 1) = 2^{t-1}(4 - e^2). \tag{4}$$

Since $2^{t-1} \wedge C_n = 1$, so $2^{t-1} \mid e + 1$. This implies that there exists $b \in \mathbb{Z}$ such that $e = b.2^{t-1} - 1$. Substituting e by its value in (4), we get:
$b \cdot C_n = 4 - e^2 = 3 - b^2.2^{2t-2} + b \cdot 2^t$, so $b(C_n + b.2^{2t-2} - 2^t) = 3$, hence $b \mid 3$ so $b = \pm 1$ or $b = \pm 3$. Since $t \geq 7$, then

$$b \cdot C_n \equiv 3 \pmod{8}. \tag{5}$$

By the previous lemma, $C_n \equiv 1 \pmod{8}$. This implies by (5) that $b \equiv 3 \pmod{8}$. Since $b = \pm 1$ or ± 3 then, the only solution is $b = 3$.
Now, the formula (4) gives:
$C_n(e + 1) > 0$ and on the other hand, $2^{t-1}(4 - e^2) < 0$ since $e = 3.2^{t-1} - 1$ and $t \geq 7$. This is unacceptable. Therefore, the proof of the stability over $\mathbb{Q}$ of the polynomial $f(x) = x^2 - x + 1$ is complete. ■

References

[1] Nidal Ali, Stabilité des polynomials, *Acta Arithmetica*, **119** (2005), no. 1, 53-63. https://doi.org/10.4064/aa119-1-4

[2] M. Ayad, D. L. McQuillan, Irreducibility of the iterates of a quadratic polynomial over a field, *Acta Arithmetica*, **93** (2000), 87-97. https://doi.org/10.4064/aa-93-1-87-97

[3] L. Danielson, B. Fein, On the irreducibility of iterates of $x^n - b$, *Proceedings of the American Mathematical Society*, **130** (2001), 1589-1596. https://doi.org/10.1090/s0002-9939-01-06258-x

[4] R. W. K. Odoni, On the prime divisors of sequence $W_{n+1} = 1 + W_1 + ...W_n$, *J. London Math. Soc.*, **2-32** (1985), 1-11. https://doi.org/10.1112/jlms/s2-32.1.1

[5] N. G. Tschebotaröw, *Grundzüge der Galois'schen Theorie* (translated from Russian by H. Schwerdtfeger), Noordhoff, Groningen, 1950.

Received: March 1, 2018; Published: July 5, 2018