Generic Polynomial of Integers and Applications

Nidal Ali, Mohamed Sarrage, Hayssam Ezzaldine and Houssam Khalil

Lebanese University, Faculty of Sciences
Mathematics Department, Lebanon

Copyright © 2014 Nidal Ali, Mohamed Sarrage, Hayssam Ezzaldine and Houssam Khalil. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

Consider an algebraic number field $K$ of degree $n$, $A'_K$ is its ring of integers and a prime number $p$ inert in $K$. Let $F(u_1, \ldots, u_n, x)$ be the generic polynomial of integers of $K$. We will study in advance the stability of this polynomial and then, we will apply it in order to obtain all the monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree $d$ dividing $n$.

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

Keywords: generic polynomial, irreducibility, iteration, stability, inert prime, totally ramified

1. Introduction

Let $K$ be an algebraic number field of degree $n \geq 2$ and $p$ is a prime number. Can we find all the monic irreducible polynomials, in $\mathbb{F}_p[x]$, of degree $d$ dividing $n$? To answer to this question, we can use the generic polynomial of integers of $K$. Thus, let us define first this polynomial and state some results concerning it.

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 $u_1, \ldots, u_n$ 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

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

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 $F(u_1^*, \ldots, u_n^*, x) = [\text{Irr}(\xi^*, \mathbb{Q}, x)]^{n/t}$ where $t = [\mathbb{Q}(\xi^*): \mathbb{Q}]$. Hence, the minimal polynomial of any element of $A_K'$ can be deduced from $F(u_1, \ldots, u_n, x)$.

**Proposition 1.** Under the hypotheses of definition 1, the generic polynomial $F(u_1, \ldots, u_n, x)$ is homogeneous of degree $n$ and $L(\xi) = L(\theta)$.

**Proof.** See [1], Remark 2.

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

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.** Let $K$ is 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 $K$. 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 [17], Satz 4, p.288.

In [12], Odoni proved the stability of $x^2 - x + 1$ over $\mathbb{Q}$. Ayad and MacQuillan have obtained in [3] an effective method to test the stability of almost all monic quadratic polynomials over a field $K$. In [6], L. Danielson and B. Fein proved the stability in $\mathbb{Z}[x]$ of all irreducible polynomial of the form $x^n - c$. In the next, we will state some results concerning the irreducibility of composition of polynomials. in fact, Schur in [4] has stated his conjecture as: Let $f(x) = x^{2n} + 1$ and $g(x)$ is a monic polynomial of degree $m$ that has distinct integer roots 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 [8], for $n = 1$ in the book of G. Pólya and G. Szegő [13], for $n = 2$ by H. Ille in [10] and for $n \leq 3$ in a more general form by A Brauer, R. Brauer and H. Hopf in [5].

H. L. Dorwat and O. Ore have obtained in [7] some results to the irreducibility of $f \circ g(x)$ for certain polynomials $f(x)$ of second and fourth degree and for $g(x)$ having distinct roots in an imaginary quadratic field. In [18], U. Wegner has proved that if $f(x) = x^4 + d, d \geq 1, d \not\equiv 3 \pmod{4}$ and $g(x)$ is is a monic polynomial of degree $m > 5$ that has distinct integer roots then, $f \circ g(x)$ is irreducible over $\mathbb{Q}$. Seres [14], [16] has proved that if the roots of $f(x)$ are complex units of a cyclotomic field and $g(x)$ has more that $\left\lceil \frac{\deg g}{2}, 5 \right\rceil$ distinct roots, then $f \circ g(x)$ is irreducible over $\mathbb{Q}$. He also proved in [15] that if $f(x)$ is cyclotomic polynomial, then $f \circ g(x)$ is reducible over $\mathbb{Q}$, if and only if,
Generic polynomial of integers and applications

\[ f(x) = x^4 - x^2 + 1 \text{ and } g(x) = (x + a)(x + a + 1)(x + a + 2), a \in \mathbb{Z}, \]
thus proving Schur’s conjecture in a more general form.

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

**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 \( \alpha \) of \( K \setminus \mathbb{Q} \) such that \( K = \mathbb{Q}(\alpha) \) and the minimal polynomial of \( \alpha \) 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 \( \mathbb{Z}[u_1, \ldots, u_n, x] \).

This result is satisfied by any number field \( K \) as Galois extension of \( \mathbb{Q} \) and of prime degree \( n \), because in this case, every prime number \( p \) of \( \mathbb{Z} \), ramified in \( K \), is totally ramified.

**Theorem 2.** Let \( K = \mathbb{Q}(\theta) \) be an algebraic number field, where \( \theta \) is a root in \( \mathbb{Q} \) of an irreducible polynomial in \( \mathbb{Z}[x] \) of the form \( f(x) = x^n - c \) then:

i) There exist infinitely many \( \alpha \) of \( K \setminus \mathbb{Q} \) such that \( K = \mathbb{Q}(\alpha) \) and the minimal polynomial of \( \alpha \) 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 \( \mathbb{Z}[u_1, \ldots, u_n, x] \).

Note that, if \( F(u_1, \ldots, u_n, x) \) is stable over \( \mathbb{Q}(u_1, \ldots, u_n) \) then it is not necessary that we can find one or infinitely many \( \alpha \) in \( K \) such that \( K = \mathbb{Q}(\alpha) \) and the minimal polynomial of \( \alpha \) is stable over \( \mathbb{Q} \).

**Proposition 2.** In general, i.e. for an algebraic number field of degree \( n \) we have \( F_2(u_1, \ldots, u_n, x) = F \circ F(u_1, \ldots, u_n, x) \) is irreducible in \( \mathbb{Z}[u_1, \ldots, u_n, x] \).

**Proof.** See [1]. Proposition 1.

**CONJECTURE.**

For instance, the stability of \( F(u_1, \ldots, u_n, x) \) of a number field of degree \( n \) is not done. Thus, it will be interesting if one can prove it.

The following theorem is due to Kummer. It will be used to factorize the prime numbers of \( \mathbb{Z} \) in \( A'_K \) as product of prime ideals.

**Theorem 3.** Let \( K = \mathbb{Q}(\theta) \) be an algebraic number field of degree \( n \), \( f(x) = \text{Irr}(\theta, \mathbb{Q}, x) \), \( A'_K \) is its ring of integers. Knowing that \( \mathbb{Z} \subseteq \mathbb{Z}[\theta] \subseteq A'_K \) and \( \Delta_\theta = I(\theta)^2 D \), let \( p \) be any prime number in \( \mathbb{Z} \) such that \( p \nmid I(\theta) \), where \( I(\theta) \) is defined to be the index of \( \theta \). It is in fact the order of the quotient group \( A'_K/\mathbb{Z}[\theta] \). The following statements are equivalent,

1) \( f(x) \equiv f_1(x)^{e_1} \cdots f_r(x)^{e_r} \pmod{p} \) the factorization of \( f(x) \) as product of irreducible factors in \( \mathbb{F}_p[x] \).
2) $pA'_K = \mathcal{P}'_1 \cdots \mathcal{P}'_r$, where $\mathcal{P}'_i = <p, f_i(\theta)>$ the prime ideal generated in $A'_k$, by $p$ and $f_i(\theta)$. (This means that we have to factorize $f(x)$ modulo $p$, in order to obtain the factorization of $pA'_K$).


This theorem can be applied only when $p \nmid I(\theta)$. The following theorem shows us how to verify if $p$ divise $I(\theta)$ or not.

**Theorem 4.** Let $K$ be a number field of degree $n$. $\theta$ is a primitive element of $K$ over $\mathbb{Q}$ and $f(x) = \text{Irr}(\theta, \mathbb{Q}, x)$. We can write,

$$f(x) = \prod_{i=1}^{t} f_i(x)^{e_i} + p.h(x)$$

where all the $f_i(x)$ are irreducible over $\mathbb{F}_p$ and $\deg h < \deg f$. Then, the following statements are equivalent:

i) $p \mid I(\theta)$.

ii) There exists $i \in \{1, \ldots, t\}, e_i \geq 2$ and $f_i(x) \mid h(x)$ in $\mathbb{F}_p[x]$.

**Proof.** See [9], Art. 95, p. 172.

**Remark 1.** Under the same hypotheses of the previous theorem and if $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ is $p$-eisenstein polynomial then, $p$ does not divide $I(\theta)$, which means, by theorem 3 that, $p$ is totally ramified in $K$. In addition, if $f(x)$ is $p^r$-eisenstein for some $r \wedge n = 1$ (that is $p^r$ divides $a_0, \ldots, a_{n-1}$ and $p^{r+1}$ does not divide $a_0$) then, by [1] Lemme 4, $p$ is also totally ramified in $K$.

2. **Main results**

Someone has asked if we can combine theorem 1 and theorem 2 to be one result. In other word, let $K = \mathbb{Q}(\theta)$ be a number field, where $\theta$ is a root in $\mathbb{Q}$ of an irreducible polynomial in $\mathbb{Z}[x]$ of the form $f(x) = x^n - c$ then, according to Kummer’s theorem and the factorization of $\text{Irr}(\theta, \mathbb{Q}, x)$ modulo prime numbers, can we always find a prime number $p$ totally ramified in $K$?

The following theorem contains the answer to this question and then, theorem 1 and theorem 2 are independent.

**Theorem 5.** Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree $n$, where $\theta$ is satisfied by the equation $\theta^n = c$ for some $c \in \mathbb{Z}$ then, it is not necessary that there exists a prime number $p$ in $\mathbb{Z}$ that is totally ramified in $A'_K$.

**Proof.** By remark 1, the integer $n$ must be greater than 6, in order to show that all the primes $p$ in $\mathbb{Z}$ are not totally ramified in $K$. Let

$$f(x) = \text{Irr}(\theta, \mathbb{Q}, x) = x^6 - 5^27^3 = x^6 - 8575.$$ 

The discriminant $\Delta_\theta$ of the basis $\{1, \theta, \ldots, \theta^5\}$ of $\mathbb{Z}[\theta]$ over $\mathbb{Z}$ is

$$\Delta_\theta = \pm 6^6(5^27^3)^5 = \pm 2^63^65^{10}7^{15}.$$
Since, \( p \) ramifies in \( K \) if and only if \( p \) divides the absolute discriminant \( D \) of \( K \), it follows that the only primes that can be ramified in \( K \) are \( \{2, 3, 5, 7\} \). We will prove that all these primes are not totally ramified.

For 2. We have \( f(x) \equiv (x + 1)^2(x^2 + x + 1)^2 \pmod{2} \). On the other hand we can write \( f(x) = (x + 1)^2(x^2 + x + 1)^2 + 2(-2x^5 - 4x^4 - 5x^3 - 4x^2 - 2x - 4288) \) which means that

\[
f(x) = f_1(x)^2 f_2(x)^2 + 2 h_1(x)
\]

where \( h_1(x) = x^3 \) in \( \mathbb{F}_2[x] \). A simple calculation shows that \( (x + 1) \) and \( (x^2 + x + 1) \) do not divide \( h_1(x) \) in \( \mathbb{F}_2[x] \). This implies, by theorem 4 that, \( 2 \nmid I(\theta) \). Thus, by theorem 3, we have \( 2A'_K = P_1^2P_2^2 \), where \( P_1 =< 2, \theta + 1 >, \ P_2 =< 2, \theta^2 + \theta + 1 >. \) Hence, that 2 is not totally ramified in \( K \).

For 3. \( f(x) \equiv (x + 1)^3(x + 2)^3 \pmod{3} \). Thus, \( f(x) = (x + 1)^3(x + 2)^3 + 3(-3x^5 - 11x^4 - 21x^3 - 22x^2 - 12x - 2861) \) so

\[
f(x) = f_3(x)^4 f_2(x)^3 + 3 h_2(x)
\]

where \( h_2(x) = x^4 + 2x^2 + 1 \) in \( \mathbb{F}_3[x] \). We can easily verify that \( (x + 1) \) and \( (x + 2) \) do not divide \( h_2(x) \) in \( \mathbb{F}_3[x] \). This implies, by theorem 4 that, \( 3 \nmid I(\theta) \). Thus, by theorem 3, we have \( 3A'_K = P_3^3P_4^3 \), where \( P_3 =< 3, \theta + 1 >, P_4 =< 3, \theta^2 + 2 >. \) Hence, 3 is not totally ramified in \( K \).

For 5. We can write \( f(x) = x^6 + 5(-5.7^3) \). Applying theorem 4, we get \( 5 \mid I(\theta) \) so we can not apply theorem 3 which means that, we have to look for another primitive element \( \alpha \) of \( K \) over \( \mathbb{Q} \). Indeed, \( \theta^3 = 35\sqrt{7} \). Let

\[
\alpha = \frac{\theta^3}{5} + \theta.
\]

This implies that \( \theta \) is root of

\[
f(y) = y^6 - 5^2.7^3 \text{ and } g(y) = \frac{y^3}{5} + y - \alpha.
\]

Applying the resulting polynomial of \( f(y) \) and \( g(y) \) we obtain that \( \alpha \) is root of \( M(x) = \text{Res}_y(y^6 - 5^2.7^3, \frac{y^3}{5} + y - x) = x^6 - 1029x^4 + 342657x^2 - 4153872 \) which is irreducible over \( \mathbb{Q} \) so \( M(x) = \text{Irr}(\alpha, \mathbb{Q}, x) \). Thus, \( K = \mathbb{Q}(\theta) = \mathbb{Q}(\alpha) \).

After calculation we have \( M(x) \equiv (x^2 + 2)^3 \pmod{5} \) and we write \( M(x) = (x^2 + 2)^3 + 5(-207x^3 + 68529x^2 - 8307736) = f_5(x)^3 + 5 h_3(x) \). In addition, \( (x^2 + 2) \) does not divide \( h_3(x) \) in \( \mathbb{F}_5[x] \) so \( 5 \nmid I(\alpha) \). By theorem 3, \( 5A'_K = P_5^3 \), where \( P_5 =< 5, \alpha^2 + 2 >. \) This implies that 5 is not totally ramified in \( K \).

For 7, \( f(x) = x^6 + 7(-5^2.7^2) \). By theorem 4, \( 7 \mid I(\theta) \), so we can not apply theorem 3. We have \( \theta^2 = 7\sqrt{25} \). Let

\[
\lambda = \frac{\theta^2}{7} + \theta.
\]
Hence θ is root of
\[ f(y) = y^6 - 5^2 \cdot 7^3 \] and \( \ell(y) = \frac{y^2}{7} + y - \lambda \).

In similar manner, λ is root of \( N(x) = \text{Res}_y(y^6 - 5^2 \cdot 7^3, \frac{y^2}{7} + y - x) = x^6 - 50x^3 - 1575x^2 - 7350x - 7950 \) which is irreducible so \( N(x) = \text{Irr}(\lambda, \mathbb{Q}, x) \). This implies that, \( K = \mathbb{Q}(\theta) = \mathbb{Q}(\lambda) \).

After calculation we have \( N(x) \equiv (x^3 + 3)^2 \) (mod 7) and then we write \( N(x) = (x^3 + 3)^2 + 7(-8x^3 - 225x^2 - 1050x - 1137) = f_6(x)^2 + 7.h_3(x) \). Since the polynomial \( (x^3 + 3) \) does not divide \( h_4(x) \) in \( \mathbb{F}_7[x] \), it follows that \( 7 \nmid I(\lambda) \). By theorem 3, \( 7A'_K = \mathcal{P}_6^2 \), where \( \mathcal{P}_6 = < 7, \lambda^3 + 3 > \). We also deduce that 7 is not totally ramified in \( K \). Therefore the required result follows.

In the next, we denote by \( K \) to be a number field of degree \( n \), \( A'_K \) its ring of integers, \( p \) is a prime number inert in \( K \) (that is the ideal \( pA'_K \) remains prime in \( A'_K \)). We also denote by \( \{w_1, ..., w_n\} \) to be a basis of \( A'_K, u_1, ..., u_n \) are \( n \) variables algebraically independent over \( K, \xi = u_1.w_1 + ... + u_n.w_n \) and \( F(u_1, ..., u_n, x) = \text{Irr}(\xi, L, x) \) the generic polynomial of \( A'_K \) of integers of \( K \).

Since \( p \) is inert in \( K \), it follows that, \( [A'_K/pA'_K : \mathbb{F}_p] = n \) and then \( \{\overline{w_1}, ..., \overline{w_n}\} \) is a basis of \( A'_K/pA'_K \) as \( \mathbb{F}_p \)-vector space of dimension \( n \). In similar manner, we define the generic polynomial of \( A'_K/pA'_K \) by:
\[
G(u_1, ..., u_n, x) = \text{Irr}(\eta, M, x)
\]
where \( \eta = u_1.\overline{w_1} + ... + u_n.\overline{w_n} \) and \( M = \mathbb{F}_p(u_1, ..., u_n) \).

We will apply the generic polynomial \( G \) of \( A'_K/pA'_K \) to find all the monic irreducible polynomials modulo \( p \) of degree \( d \) dividing \( n \).

**Lemma 2.** Let \( K \) be a number field of degree \( n \), \( A'_K \) is its ring of integers, \( F(u_1, ..., u_n, x) \) the generic polynomial of integers of \( K \) and \( p \) is a prime of \( \mathbb{Z} \) having the decomposition in \( A'_K \) as:
\[
pA'_K = \prod_{i=1}^{t} \mathcal{P}_i^{e_i}.
\]
Then we have:
\[
F(u_1, ..., u_n, x) = \prod_{i=1}^{t} F_i(u_1, ..., u_n, x)^{e_i} + p.G(u_1, ..., u_n, x)
\]
where the \( F_i(u_1, ..., u_n, x) \) are irreducible over \( \mathbb{F}_p \), monic and \( G(u_1, ..., u_n, x) \) is not divisible by any factor \( F_i(u_1, ..., u_n, x) \) in \( \mathbb{F}_p[u_1, ..., u_n, x] \).

**Proof.** See ([9], Theorem 1, p. 137).

**Proposition 3.** The polynomial \( F(u_1, ..., u_n, x) \) is congruent to \( G(u_1, ..., u_n, x) \) modulo \( p \).
Proof. The prime number $p$ is inert in $K$ so, by lemma 2, the polynomial $F$ remains irreducible in $\mathbb{F}_p[u_1, ..., u_n, x]$. Since $F(u_1, ..., u_n, \eta) \equiv 0 \pmod{p}$, it follows that $G$ divides $F$ in $\mathbb{F}_p[u_1, ..., u_n, x]$. Thus,

$$F(u_1, ..., u_n, x) \equiv G(u_1, ..., u_n, x) \pmod{p}.$$ 

Let,

$$E = \{ f(x) \in \mathbb{F}_p[x] \text{ monic of degree } n \text{ such that there exists } d \mid n, g(x) \in \mathbb{F}_p[x], \text{ monic irreducible of degree } d \text{ and } f(x) = g(x)^{n/d} \}.$$ 

and the mapping,

$$\psi : \mathbb{F}_p^n \longrightarrow E$$

defined by,

$$\psi(u_1^*, ..., u_n^*) = G(u_1^*, ..., u_n^*, x)$$

which is equal to $[\text{Irr}(\eta^*, \mathbb{F}_p, x)]^{n/d}$ where $\eta^* = u_1^*\bar{w}_1 + ... + u_n^*\bar{w}_n$, $d = [\eta^* : \mathbb{F}_p]$.

Let $R$ be the equivalence relation defined on $\mathbb{F}_p^n$ by:

$$(u_1^*, ..., u_n^*)R(v_1^*, ..., v_n^*) \iff \psi(u_1^*, ..., u_n^*) = \psi(v_1^*, ..., v_n^*).$$

Theorem 6. The application $\psi$ is surjective and defines a bijection from $\mathbb{F}_p^n/R$ onto $E$.

Proof. Let $f(x) \in E$, there exists a monic irreducible polynomial $g(x) \in \mathbb{F}_p[x]$, of degree $d$ such that $f(x) = g(x)^{n/d}$. Let $\alpha$ is a root of $g(x)$. This implies that there exists $(u_1^*, ..., u_n^*) \in \mathbb{F}_p^n$ such that $\alpha = u_1^*\bar{w}_1 + ... + u_n^*\bar{w}_n$. Hence, $f(x) = G(u_1^*, ..., u_n^*, x)$, which implies that the application $\psi$ is surjective. Since $R$ is equivalence relation it follows that, we can deduce from the application $\psi$, a bijection from $\mathbb{F}_p^n/R$ onto $E$. 

Remark 2. The equivalence relation $R$ can also be defined as: For all $u^* = (u_1^*, ..., u_n^*)$ and $v^* = (v_1^*, ..., v_n^*)$ in $\mathbb{F}_p^n$, $u^*Rv^*$, if and only if, there exists $j \in \{0, 1, ..., n - 1\}$ such that

$$\sum_{i=1}^{n} v_i^* \bar{w}_i = (\sum_{i=1}^{n} u_i^* \bar{w}_i)^{p^j}.$$

Definition 3. The equivalence class of $u^*$ according to $R$ is defined to be orbit of $u^*$ and denoted by: $\text{Orb}(u^*)$.

Thus, we have

$$\text{Orb}(u^*) = \{ v^* \in \mathbb{F}_p^n \text{ such that } \psi(u^*) = \psi(v^*) \}.$$
which is equal to
\[ \{ v^* \in \mathbb{F}_p^n \text{ such that there exists } j = 0, 1, \ldots, n-1 \text{ and } \sum_{i=1}^n v_i^*.w_i = (\sum_{i=1}^n u_i^*.w_i)^p \}. \]

This implies that \( \sum_{i=1}^n u_i^*.w_i \) and \( \sum_{i=1}^n v_i^*.w_i \) are conjugates. We deduce that the cardinal of the orbit is \(|\text{Orb}(u^*)| = d|\). The other elements \( (\sum_{i=1}^n u_i^*.w_i)^p = \sum_{i=1}^n l_i(u^*).w_i \) where the \( l_i \) are linear forms on \( \mathbb{F}_p \). Consider the application:
\[ \varphi : \mathbb{F}_p^n \longrightarrow \mathbb{F}_p^n \]
defined by \( \varphi(u^*) = (l_1(u^*), \ldots, l_n(u^*)) \). Then,
\[ \text{Orb}(u^*) = \{ \varphi^i(u^*), i = 0, \ldots, n-1 \} \]
where \( \varphi^i = \varphi \circ \ldots \circ \varphi \), \( i \) times, is defined to be the \( i^{th} \) iterate of \( \varphi \).

**Example.** Let \( K = \mathbb{Q}(i) \), \( A'_K \) is its ring of integers, so \( \{1, i\} \) is a basis of \( A'_K \) and each prime number \( p \equiv -1 \pmod{4} \) is inert in \( K \). Let \( \eta = u_1.\overline{1} + u_2.\overline{I} \), then \( \{1, \overline{i}\} \) is a basis of \( A'_K/pA'_K \) over \( \mathbb{F}_p \) and
\[ G(u_1, u_2, x) = x^2 - 2u_1x + u_1^2 + u_2^2 \]
for all \( (u_1^*, u_2^*) \in \mathbb{F}_p^2 \), where \( \eta^* = u_1^*.\overline{1} + u_2^*.\overline{I} \) and \( \eta^{*p} = u_1^*.\overline{1} - u_2^*.\overline{I} \). Thus, we have:
\[ \text{Orb}((u_1^*, u_2^*)) = \{ (u_1^*, -u_2^*), (u_1^*, u_2^*) \}. \]

Hence, every element \( (u_1^*, u_2^*) \) such that \(|\text{Orb}(u_1^*, u_2^*)| = 2 \) gives a quadratic irreducible polynomial over \( \mathbb{F}_p \). The other elements \( (u_1^*, u_2^*) \) are whose have \(|\text{Orb}(u_1^*, u_2^*)| = 1 \), so \( u_2^* = 0 \), they are squares of polynomials of first degree.

**Remark 3.** It is important to bring back the calculation of the orbit easier. Indeed, it is sufficient to calculate only \( \varphi(u^*) = (l_1(u^*), \ldots, l_n(u^*)) \). In fact, we find \( \varphi^i(u^*) \) by iterating \( (l_1(u^*), \ldots, l_n(u^*)) \), \( i \)-times.

Now we can say that each monic polynomial of degree \( n \), power of an irreducible polynomial modulo \( p \), can be found, in a unique way, by taking from each orbit one of its elements.

**Remark 4.** Theorem 6 is false if we take \( \{w_1, \ldots, w_n\} \) basis of \( K \) in \( A'_K \) but not a basis \( A'_K \). Indeed, let \( K = \mathbb{Q}(\sqrt{5}) \), \( p = 2 \), then \( p \) is inert in \( K \) and \( \{1, \sqrt{5}\} \) is a basis of \( K \) but not of \( A'_K \). Let \( \eta = u_1.\overline{1} + u_2.\sqrt{5} \). In this case, \( G(u_1, u_2, x) = x^2 + u_1^2 + u_2^2 \). The polynomial \( f(x) = x^2 + x + 1 \in E \) and it is not image of any element of \( \mathbb{F}_2^2 \). This implies that the application \( \psi \) is not surjective in this case.
3. Applications

Application 1: \((p = 5, n = 2)\)

Let \(p = 5, K = \mathbb{Q}(\sqrt{2})\). Since \(p \equiv 5 \pmod{8}\), it follows that, \(p\) is inert in \(K\).
We have, \(\eta = u_1 \bar{\tau} + u_2 \sqrt{2} \) and then
\[
G(u_1, u_2, x) = x^2 - 2u_1 x + u_1^2 - 2u_2^2.
\]

There are 25 specializations \((u_1^*, u_2^*)\) in \(\mathbb{F}_5^2\), \(\eta^* = u_1^* \bar{\tau} + u_2^* \sqrt{2}\) and \(\eta^{*2} = u_1^* \bar{\tau} - u_2^* \sqrt{2}\). Thus, we have:
\[
Orb((u_1^*, u_2^*)) = \{(u_1^*, -u_2^*); (u_1^*, u_2^*)\}.
\]

The 5 specializations \((u_1^*, 0)\), where \(u_1^* \in \mathbb{F}_5\) give the polynomials \(G(u_1^*, 0, x) = (x - u_1^*)^2\). The other specializations give 10 quadratic irreducible polynomials over \(\mathbb{F}_5\):

<table>
<thead>
<tr>
<th>Specializations in (\mathbb{F}_5^2)</th>
<th>Irreducible polynomials over (\mathbb{F}_5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0, 0)</td>
<td>(x^4)</td>
</tr>
<tr>
<td>(1, 0)</td>
<td>((x + 4)^2)</td>
</tr>
<tr>
<td>(2, 0)</td>
<td>((x + 3)^2)</td>
</tr>
<tr>
<td>(3, 0)</td>
<td>((x + 2)^2)</td>
</tr>
<tr>
<td>(4, 0)</td>
<td>((x + 1)^2)</td>
</tr>
<tr>
<td>(0, -2), (0, 2)</td>
<td>(x^4 + 2)</td>
</tr>
<tr>
<td>(0, -1), (0, 1)</td>
<td>(x^2 + 3)</td>
</tr>
<tr>
<td>(2, -2), (2, 2)</td>
<td>(x^2 + x + 1)</td>
</tr>
<tr>
<td>(2, -1), (2, 1)</td>
<td>(x^2 + x + 2)</td>
</tr>
<tr>
<td>(-1, -2), (-1, 2)</td>
<td>(x^2 + 2x + 3)</td>
</tr>
<tr>
<td>(-1, -1), (-1, 1)</td>
<td>(x^2 + 2x + 4)</td>
</tr>
<tr>
<td>(1, -2), (1, 2)</td>
<td>(x^2 + 3x + 3)</td>
</tr>
<tr>
<td>(1, -1), (1, 1)</td>
<td>(x^2 + 3x + 4)</td>
</tr>
<tr>
<td>(-2, -2), (-2, 2)</td>
<td>(x^2 + 4x + 1)</td>
</tr>
<tr>
<td>(-2, -1), (-2, 1)</td>
<td>(x^2 + 4x + 2)</td>
</tr>
</tbody>
</table>

Application 2: \((p = 3, n = 3)\)

Let \(p = 3, K = \mathbb{Q}(\theta)\), where \(\theta\) is root of the polynomial \(f(x) = x^3 - x + 1\).
\(\Delta_\theta = -23\) is square free so \(\{1, \theta, \theta^2\}\) is a basis of \(A_K\) and then \(I(\theta) = 1\). By theorem 3, the prime \(3\) is inert in \(K\). We have, \(\eta = a \bar{\tau} + b \sqrt{2} + c \bar{\tau}^2\), where \(a, b, c\) are three algebraically independent variables. To make calculation easier, we find \(F(a, b, c, x)\) and then we find \(G(a, b, c, x)\) by reducing modulo \(p\). Indeed, \(F(a, b, c, x) = \text{Irr}(\xi, L, x) = \text{Char}(\xi, L(\xi)/L, x)\). By proposition 1, we have \(L(\xi) = L(\theta)\) so \(F(a, b, c, x) = \text{Char}(\xi, L(\theta)/L, x) = |xI_3 - M|\), where
\[
M = \begin{pmatrix}
a & -c & -b \\
b & a + c & b - c \\
c & b & a + c
\end{pmatrix}
\]
Since \( F(a, b, c, x) \equiv G(a, b, c, x) \pmod{3} \), it follows that 
\[
G(a, b, c, x) = x^3 + cx^2 + (2b^2 + ac + c^2)x + 2a^3 + b^3 + 2c^3 + 2bc^2 + ab^2 + a^2c + 2ac^2.
\]

In the next step, we find the orbit. By remark 3, it is enough to find only \( \varphi(a, b, c) \). In fact, \( \eta = a.\overline{1} + b.\overline{\theta} + c.\overline{\theta^2} \) so \( \eta^3 = a.\overline{1} + b.\overline{\theta^3} + c.\overline{\theta^6} = a.\overline{1} + b(\overline{\theta} - 1) + c(\overline{\theta^2} + \overline{\theta} + 1) \). Hence,
\[
\eta^3 = (a - b + c).\overline{1} + (b + c)\overline{\theta} + c\overline{\theta^2}
\]
which means that \( \varphi(a, b, c) = (a - b + c, b + c, c) \) and then, by iteration we deduce that
\[
Orb(a, b, c) = \{(a, b, c); (a - b + c, b + c, c); (a + b + c, b - c, c)\}.
\]

The number of specializations in \( \mathbb{F}_3 \) is 27. Indeed, we have 3 specializations that give 3 polynomials of degree 3 power of polynomials of first degree. The other 24 specializations will give 8 irreducible polynomials of degree 3 over \( \mathbb{F}_3 \).

<table>
<thead>
<tr>
<th>Specializations in ( \mathbb{F}_3^3 )</th>
<th>Irreducible polynomials over ( \mathbb{F}_3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0, 0, 0)</td>
<td>( x^3 )</td>
</tr>
<tr>
<td>(1, 0, 0)</td>
<td>( (x + 2)^3 )</td>
</tr>
<tr>
<td>(2, 0, 0)</td>
<td>( (x + 1)^3 )</td>
</tr>
<tr>
<td>(0, 0, 1), (1, 1, 1), (1, 2, 1)</td>
<td>( x^3 + x^2 + x + 2 )</td>
</tr>
<tr>
<td>(0, 0, 2), (2, 2, 2), (2, 1, 2)</td>
<td>( x^3 + 2x^2 + x + 1 )</td>
</tr>
<tr>
<td>(0, 1, 0), (2, 1, 0), (1, 1, 0)</td>
<td>( x^3 + 2x + 1 )</td>
</tr>
<tr>
<td>(0, 1, 1), (0, 2, 1), (2, 0, 1)</td>
<td>( x^3 + x^2 + 2 )</td>
</tr>
<tr>
<td>(0, 1, 2), (1, 0, 2), (0, 2, 2)</td>
<td>( x^3 + 2x^2 + 1 )</td>
</tr>
<tr>
<td>(0, 2, 0), (1, 2, 0), (2, 2, 0)</td>
<td>( x^3 + 2x + 2 )</td>
</tr>
<tr>
<td>(1, 0, 1), (2, 1, 1), (2, 2, 1)</td>
<td>( x^3 + x^2 + 2x + 1 )</td>
</tr>
<tr>
<td>(1, 1, 2), (2, 0, 2), (1, 2, 2)</td>
<td>( x^3 + 2x^2 + 2x + 2 )</td>
</tr>
</tbody>
</table>

**Application 3:** \( (p = 2, n = 4) \)

For \( p = 2 \), let us take \( K = \mathbb{Q}(\theta) \), where \( \theta \) is root of the polynomial \( f(x) = x^4 + x + 1 \). We have \( I(\theta) = 1 \). Indeed, \( \Delta_\theta = 229 \) is square free so \( A'_K = \mathbb{Z}[\theta] \), which means that \( \{1, \theta, \theta^2, \theta^3\} \) is a basis of \( A'_K \). Again by theorem 3, the prime 2 is inert in \( K \) because \( f(x) \) remains irreducible modulo 2. We have, \( \eta = a.\overline{1} + b.\overline{\theta} + c.\overline{\theta^2} + d.\overline{\theta^3} \), where \( a, b, c, d \) are four algebraically independent variables. \( F(a, b, c, x) = Irr(\xi, L, x) = Char(\xi, L(\xi)/L, x) = Char(\xi, L(\theta)/L, x) \). Since \( F(a, b, c, d, x) \equiv G(a, b, c, d, x) \pmod{2} \), we can directly find \( G(a, b, c, d, x) \) by reducing the matrix \( M \) modulo 2. This implies that, \( G(a, b, c, d, x) = [xI_4 - M] \), where

\[
\overline{M} = \begin{pmatrix}
a & d & c & b \\
b & a + d & c + d & b + c \\
c & b & a + d & c + d \\
d & c & b & a + d \\
\end{pmatrix}.
\]

Therefore,
Generic polynomial of integers and applications

$G(a, b, c, d, x) = x^4 + dx^3 + (a + bx + d^3)x^2 + (a^2d + c^2d + bcd + b^3 + c^3 + d^3)x + a^4 + b^4 + c^4 + d^4 + a^3d + a^2d^2 + ab^3 + ac^3 + ad^3 + bc^3 + bd^3 + cd^3 + a^2bc + abd^2 + ac^2d + b^2cd + abcd.$

Now, we have to find the orbit. Indeed, $\eta = a.\overline{1} + b\overline{\theta} + c\overline{\theta^2} + d\overline{\theta^3}$ so $\eta^2 = a.\overline{1} + b\overline{\theta}^2 + c\overline{\theta^4} + d\overline{\theta^6} = a.\overline{1} + b\overline{\theta}^2 + c(\overline{\theta} + 1) + d(\overline{\theta^3} + \overline{\theta^2})$. Hence,

$$\eta^2 = (a + c).\overline{1} + c\overline{\theta} + (b + d)\overline{\theta^2} + d\overline{\theta^3}$$

which means that $\varphi(a, b, c, d) = (a + c, b + d, d)$. By iteration we deduce that

$\text{Orb}(a, b, c, d) = \{(a, b, c, d); (a + c, b, c, d); (a + b + c + d, b + d, c + d, d); (a + b, c + d, b, d)\}$.  

The number of specializations in $\mathbb{F}_2$ is 16. Indeed, we have 2 specializations that give 2 polynomials of degree 4 power of polynomials of first degree and 2 specializations that give one polynomial of degree 4 power of an irreducible polynomial of second degree. The other 12 specializations will give 3 irreducible polynomials of degree 4 over $\mathbb{F}_2$.

<table>
<thead>
<tr>
<th>Specializations in $\mathbb{F}_2^4$</th>
<th>Irreducible polynomials over $\mathbb{F}_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(0, 0, 0, 0)$</td>
<td>$x^4$</td>
</tr>
<tr>
<td>$(1, 0, 0, 0)$</td>
<td>$(x + 1)^4$</td>
</tr>
<tr>
<td>$(0, 1, 1, 0), (1, 1, 1, 0)$</td>
<td>$(x^2 + x + 1)^2$</td>
</tr>
<tr>
<td>$(0, 0, 0, 1), (0, 0, 1, 1), (1, 1, 1, 1), (0, 1, 0, 1)$</td>
<td>$x^4 + x^3 + x^2 + x + 1$</td>
</tr>
<tr>
<td>$(0, 0, 1, 0), (1, 1, 0, 0), (0, 1, 0, 0)$</td>
<td>$x^4 + x + 1$</td>
</tr>
<tr>
<td>$(0, 1, 1, 1), (1, 1, 0, 1), (1, 0, 0, 1), (1, 0, 1, 1)$</td>
<td>$x^4 + x^4 + 1$</td>
</tr>
</tbody>
</table>

We would like to thank very much the Lebanese University for supporting this work.

References


Received: December 19, 2014; Published: February 12, 2015