Indian J. Pure Appl. Math., **51**(1): 171-177, March 2020
© Indian National Science Academy DOI: 10.1007/s13226-020-0392-x

AN IRREDUCIBILITY TEST FOR POLYNOMIALS WHOSE COEFFICIENTS ARE ALGEBRAIC INTEGERS

Gajendra Singh

Jai Narain Vyas University, Jodhpur, Rajasthan, India
e-mail: singhgajendra1729@gmail.com

(*Received* 3 *July* 2018; *after final revision* 30 *November* 2018;
accepted 10 *January* 2019)

For a non-zero algebraic integer α, let $\mathbb{Q}(\alpha)$ denote the simple extension of the field of rational numbers $\mathbb{Q}$. $\mathbb{Z}[\alpha]$ is the smallest subring of $\mathbb{Q}(\alpha)$ containing both $\mathbb{Z}$ and α. In this article, we present an account for testing irreducibility of a given polynomial with coefficients in $\mathbb{Z}[\alpha]$ over the field $\mathbb{Q}(\alpha)$.

Key words : Simple extension; algebraic integer; polynomial irreducibility.

2010 Mathematics Subject Classification : 11R04, 11R09

1. INTRODUCTION

Irreducibility tests and criteria for polynomials play very important role in the factorization of the polynomials. Testing the irreducibility of a polynomial over a field $\mathbb{F}$ is also important in determining the degree of the extension field of $\mathbb{F}$. The presence of various irreducibility tests and criteria for polynomials over field of rationals or over the ring of integers in the literature has a long history: modulo prime irreducibility test (Theorem 17.3 of [4]), Eisenstein's irreducibility criterion [2], Hilbert's irreducibility theorem [3], Cohn's irreducibility criterion [1, 5]; but, finding the analogous tests for polynomials over the fields of algebraic numbers or the rings of algebraic integers is not an easy task. In this paper we present an irreducibility test for polynomials with algebraic integer coefficients that is a generalization of the 'modulo prime irreducibility test' for polynomials with integer coefficients.

Notation 1.1 : $\mathbb{Q}(\alpha)$ is the simple extension of the field of rational numbers $\mathbb{Q}$ for an algebraic integer α. The minimal monic polynomial of α is $\Psi(x) = x^n - c_{n-1}x^{n-1} - c_{n-2}x^{n-2} - \ldots - c_0 \in$

$\mathbb{Z}[x]$. A set $\mathbb{M}$ is defined as $\mathbb{M} = \{\alpha - m : m \in \mathbb{Z}, |\Psi(m)| \text{ is prime }\}$. Here we write $\mathbb{Z}_p$ for the ring $\mathbb{Z}/p\mathbb{Z}$ of residues modulo p. $\mathbb{Z}_p[x]$ and $\mathbb{Z}[\alpha][x]$ are polynomial rings over $\mathbb{Z}_p$ and $\mathbb{Z}[\alpha]$ respectively. An integer r is called 'remainder of $\mathfrak{a} \in \mathbb{Z}[\alpha]$ divided by $(\alpha - m)$' denoted as $r = \mathfrak{a} \bmod (\alpha - m)$ if $\mathfrak{a} = (\alpha - m) \cdot \mathfrak{q} + r$ for some $\mathfrak{q} \in \mathbb{Z}[\alpha]$ and $0 \leq r < |\Psi(m)|$. We say two elements $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathbb{Z}[\alpha]$ are 'congruent modulo $(\alpha - m)$' denoted as $\mathfrak{a} \equiv \mathfrak{b} \bmod (\alpha - m)$ if $(\alpha - m)|(\mathfrak{a} - \mathfrak{b})$. All indices in superscripts are always written inside parentheses.

We prove the following theorem as the main result:

***Theorem* 1.1** — *For an element $(\alpha - m) \in \mathbb{M}$, consider the map $\theta : \mathbb{Z}[\alpha] \to \mathbb{Z}_{|\Psi(m)|}$ defined as $\theta(\mathfrak{a}) = \mathfrak{a}$ mod $(\alpha - m)$, where $\mathfrak{a} \in \mathbb{Z}[\alpha]$; consider $\mathfrak{F}(x) = \mathfrak{a}_n x^n + \mathfrak{a}_{n-1}x^{n-1} + \mathfrak{a}_{n-2}x^{n-2} + \ldots + \mathfrak{a}_0 \in \mathbb{Z}[\alpha][x]$ with $n \geq 1$ and $\overline{\mathfrak{F}(x)} = \theta(\mathfrak{a}_n)x^n + \theta(\mathfrak{a}_{n-1})x^{n-1} + \theta(\mathfrak{a}_{n-2})x^{n-2} + \ldots + \theta(\mathfrak{a}_0)x^0 \in \mathbb{Z}_{|\Psi(m)|}[x]$. If $\overline{\mathfrak{F}(x)}$ is irreducible over $\mathbb{Z}_{|\Psi(m)|}$ and $deg\overline{\mathfrak{F}(x)} = deg\mathfrak{F}(x)$, then $\mathfrak{F}(x)$ is irreducible over $\mathbb{Q}(\alpha)$.*

If $\alpha \in \mathbb{Q}$, the above Theorem becomes the usual Reduction (mod p)-test (Theorem 17.3 of [4]).

2. Preliminary Results

The following Lemma is used in the sequels:

Lemma 2.1 — $\mathbb{Z}[\alpha]/\langle \alpha - m \rangle$ is isomorphic to $\mathbb{Z}_{|\Psi(m)|}$, where $\langle \alpha - m \rangle$ denotes the ideal in $\mathbb{Z}[\alpha]$ generated by $\alpha - m$ for an integer m that is not the zero of $\Psi(x)$.

Proof : Using the fact that only the integer multiples of $|\Psi(m)|$ in the set of integers can be written as $(\alpha - m) \cdot \mathfrak{q}'$ where $\mathfrak{q}' \in \mathbb{Z}[\alpha]$, the following can easily be shown: for $\mathfrak{a} \in \mathbb{Z}[\alpha]$, there exist a unique $\mathfrak{q} \in \mathbb{Z}[\alpha]$ and $r \in \mathbb{Z}$ such that $\mathfrak{a} = (\alpha - m) \cdot \mathfrak{q} + r$ where $0 \leq r < |\Psi(m)|$. The latter implies that the function $\theta \colon \mathbb{Z}[\alpha] \to \mathbb{Z}_{|\Psi(m)|}$, such that $\theta(\mathfrak{a}) = r$; is ring homomorphism. Thus, $\mathbb{Z}[\alpha]/\langle \alpha - m \rangle$ is isomorphic to $\mathbb{Z}_{|\Psi(m)|}$ by first isomorphism theorem for rings. □

Remark 2.1 : For an integer m, $(\alpha - m)$ is a prime element of $\mathbb{Z}[\alpha]$ if and only if $|\Psi(m)|$ is a prime number.

The following two corollaries of independent interest are immediate consequences of Lemma 2.1:

Corollary 2.1 — If $(\alpha - m) \in \mathbb{M}$ and $\mathfrak{a} \in \mathbb{Z}[\alpha]$ such that $gcd(r, |\Psi(m)|) = 1$ where r is the remainder of $\mathfrak{a}$ divided by $(\alpha - m)$, then

$$\mathfrak{a}^{(|\Psi(m)|-1)} \equiv 1 \bmod (\alpha - m)$$

Corollary 2.2 — If $m \in \mathbb{Z}$ and $\mathfrak{a} \in \mathbb{Z}[\alpha]$ such that $gcd(r_0, |\Psi(m)|) = 1$ where r_0 is the remainder

of $\mathfrak{a}$ divided by $(\alpha - m)$, then

$$\mathfrak{a}^{\phi(|\Psi(m)|)} \equiv 1 \bmod (\alpha - m)$$

ϕ is Euler's totient function.

$\mathbb{Q}(\alpha)$ is a vector space of dimension n over the field $\mathbb{Q}$. For some $\mathfrak{a}' = \sum_{r=0}^{n-1} {a'}_r \alpha^r \in \mathbb{Q}(\alpha)$, we define the linear transformation $T_{\mathfrak{a}'} : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ by setting $T_{\mathfrak{a}'}(\mathfrak{t}) = \mathfrak{a}' \cdot \mathfrak{t}$. The transformation matrix $[A'_{ij}]$ of $T_{\mathfrak{a}'}$ can be written as:

$$A'_{ij} = \begin{cases} {a'}_{i-1} & \text{if} \quad j = 1 \\ \sigma_{ij} {a'}_{|i-j|} + \sum_{r=1}^{j-1} {a'}_{n-j+r} \phi_r^{(i-1)} & \text{if} \quad j \neq 1 \end{cases} \tag{1}$$

with

$$\sigma_{ij} = \begin{cases} 0 & \text{for} \quad i < j \\ 1 & \text{for} \quad i \geq j \end{cases}$$

and $\phi_s^{(r)}$ corresponding to $\Psi(x) = x^n - \sum_{i=0}^{n-1} c_i x^i$, $\forall c_i \in \mathbb{Z}$ defined as:

$$\begin{aligned} \phi_1^{(r)} &= \begin{cases} 0 & \text{for} \quad r < 0 \\ c_r & \text{for} \quad r \geq 0 \end{cases} \\ \phi_s^{(r)} &= \phi_{s-1}^{(n-1)} \phi_1^{(r)} + \phi_{s-1}^{(r-1)} \quad \text{for} \quad s \geq 2 \end{aligned} \tag{2}$$

It is well known that determinant of $[A'_{ij}]$ is norm of $\mathfrak{a}'$ (Lemma 3.8.4 of [6]), say $det[A'_{ij}] = \mathcal{N}(\mathfrak{a}')$. For $\mathfrak{a}'$ being an element of $\mathbb{Z}[\alpha]$, $det[A'_{ij}]$ is integer.

We show here that an element $\mathfrak{a} \in \mathbb{Z}[\alpha]$ is unit *iff* $|\mathcal{N}(\mathfrak{a})| = 1$. This is useful in proving the next theorem. Suppose $\mathfrak{a}$ is a unit element of $\mathbb{Z}[\alpha]$. There exists an element $\mathfrak{b} \in \mathbb{Z}[\alpha]$ such that $\mathfrak{a} \cdot \mathfrak{b} = 1$, furthermore, $|\mathcal{N}(\mathfrak{a} \cdot \mathfrak{b})| = 1 \Rightarrow |\mathcal{N}(\mathfrak{a})| \cdot |\mathcal{N}(\mathfrak{b})| = 1$. This is true if and only if $|\mathcal{N}(\mathfrak{a})| = 1$. Conversely, consider that there exists an element $\mathfrak{a} \in \mathbb{Z}[\alpha]$ such that $|\mathcal{N}(\mathfrak{a})| = 1$. Let $\mathfrak{a} = \sum_{r=0}^{n-1} a_r \alpha^r$, $\mathfrak{b}' = \sum_{r=0}^{n-1} {b_r}' \alpha^r$ and $\mathfrak{x}' = \sum_{r=0}^{n-1} {x_r}' \alpha^r$, where $\mathfrak{b}', \mathfrak{x}' \in \mathbb{Q}(\alpha)$ such that $\mathfrak{a} \cdot \mathfrak{x}' = \mathfrak{b}'$. Using relation $\alpha_n^n = \sum_{r=0}^{n-1} \phi_1^r \alpha_n^r$, one can easily prove that $\alpha^s = \sum_{r=0}^{n-1} \phi_{s-(n-1)}^{(r)} \alpha^r$ for $s \geq n$. Using the latter, we have:

$$\begin{aligned} \left(\sum_{r=0}^{n-1} a_r \alpha^r \right) \left(\sum_{r=0}^{n-1} {x_r}' \alpha^r \right) &= \sum_{i=1}^{n} \sum_{j=1}^{n} A_{ij} {x'}_{j-1} \alpha^{i-1} \\ \Rightarrow \sum_{r=0}^{n-1} {b_r}' \alpha^r &= \sum_{i=1}^{n} \sum_{j=1}^{n} A_{ij} {x'}_{j-1} \alpha^{i-1} \end{aligned} \tag{3}$$

$[A_{ij}]$ is the transformation matrix for $\mathfrak{a}$ corresponding to $T_{\mathfrak{a}}$.

Now consider $b_0 = 1$ and $b_r = 0$ for $1 \leq r \leq n-1$ *i.e.* $\mathfrak{a} \cdot \mathfrak{x}' = 1$. Equating the coefficients of respective powers of α on both sides of equation (3), we get a set of n linear equations for n variables $\{x'_0, x'_1, x'_2, \ldots, x'_{n-1}\}$. By Cramer's rule

$$x'_j = \frac{\text{co-factor of } A_{1(j+1)}}{\det[A_{ij}]}$$

Since $|\mathcal{N}(\mathfrak{a})| = 1 \Rightarrow |\det[A_{ij}]| = 1$, x'_j is an integer $\forall j \in \{0, 1, 2 \ldots n-1\}$, and thus $\mathfrak{x}' \in \mathbb{Z}[\alpha]$. Therefore $\mathfrak{a}$ is a unit element of $\mathbb{Z}[\alpha]$.

***Theorem* 2.1** — *Every non-zero element of $\mathbb{Z}[\alpha]$ can be expressed in the form $\mathfrak{b}_1^{n_1} \cdot \mathfrak{b}_2^{n_2} \cdot \mathfrak{b}_3^{n_3} \cdot \ldots \cdot \mathfrak{b}_r^{n_r} \cdot \mathfrak{v}_1$ where $\mathfrak{b}$'s are elements of $\mathbb{M}$ and $\mathfrak{v}_1$ is a non-zero element of $\mathbb{Z}[\alpha]$ such that $\mathfrak{x} \nmid \mathfrak{v}_1$, $\forall \mathfrak{x} \in \mathbb{M}$. Furthermore, if $\mathfrak{b}_1^{n_1} \cdot \mathfrak{b}_2^{n_2} \cdot \mathfrak{b}_3^{n_3} \cdot \ldots \cdot \mathfrak{b}_r^{n_r} \cdot \mathfrak{v}_1 = \mathfrak{c}_1^{m_1} \cdot \mathfrak{c}_2^{m_2} \cdot \mathfrak{c}_3^{m_3} \cdot \ldots \cdot \mathfrak{c}_s^{m_s} \cdot \mathfrak{v}_2$ where the $\mathfrak{c}$'s are elements of $\mathbb{M}$, $\mathfrak{v}_2$ is a non-zero element of $\mathbb{Z}[\alpha]$ such that $\mathfrak{x} \nmid \mathfrak{v}_2$, $\forall \mathfrak{x} \in \mathbb{M}$ and neither any two of the $\mathfrak{b}$'s nor any two of the $\mathfrak{c}$'s are associates; then $r = s$ and after renumbering the $\mathfrak{c}$'s we have $n_i = m_i$, $\mathfrak{b}_i$ is associate of $\mathfrak{c}_i$ for $i = 1, 2, 3, \ldots, r$, and $\mathfrak{v}_1$ is associate of $\mathfrak{v}_2$.*

PROOF : For any non-zero element $\mathfrak{a}$ of $\mathbb{Z}[\alpha]$, we consider two mutually exclusive cases:

1. $\mathfrak{x} \nmid \mathfrak{a}$, $\forall \mathfrak{x} \in \mathbb{M}$
2. $\exists \mathfrak{x} \in \mathbb{M}$ such that $\mathfrak{x} | \mathfrak{a}$

If (1) is true for some non-zero element $\mathfrak{a}_0 \in \mathbb{Z}[\alpha]$, then $\mathfrak{a}_0$ can trivially be expressed in the given form. In case (2) is true for $\mathfrak{a}_0$, we can express $\mathfrak{a}_0 = \mathfrak{b}_1^{n_1} \mathfrak{a}_1$ for some $\mathfrak{b}_1 \in \mathbb{M}$ such that $\mathfrak{b}_1 \nmid \mathfrak{a}_1$ and $\mathfrak{a}_1$ is a non-zero element of $\mathbb{Z}[\alpha]$. Similarly, if (1) is true for $\mathfrak{a}_1$, then $\mathfrak{b}_1^{n_1} \mathfrak{a}_1$ is in the given form but in case (2) is true for $\mathfrak{a}_1$, we can further express $\mathfrak{a}_1 = \mathfrak{b}_2^{n_2} \mathfrak{a}_2$ for some $\mathfrak{b}_2 \in \mathbb{M}$ such that $\mathfrak{b}_2 \nmid \mathfrak{a}_2$ and $\mathfrak{a}_2$ is a non-zero element of $\mathbb{Z}[\alpha]$. Continuing this procedure we obtain $\mathfrak{a}_0 = \mathfrak{b}_1^{n_1} \cdot \mathfrak{b}_2^{n_2} \cdot \mathfrak{b}_3^{n_3} \cdot \ldots \cdot \mathfrak{b}_r^{n_r} \cdot \mathfrak{a}_r$ for some $r \in \mathbb{N}$ and $\mathfrak{a}_r$ being a non-zero element of $\mathbb{Z}[\alpha]$. Now we make an assumption that for each $r \in \mathbb{N}$, there exists at least one element $\mathfrak{x} \in \mathbb{M}$ such that $\mathfrak{x} | \mathfrak{a}_r$. Clearly, $|\mathcal{N}(\mathfrak{a}_0)| = |\mathcal{N}(\mathfrak{b}_1)|^{n_1} \cdot |\mathcal{N}(\mathfrak{b}_2)|^{n_2} \cdot |\mathcal{N}(\mathfrak{b}_3)|^{n_3} \cdot \ldots \cdot |\mathcal{N}(\mathfrak{b}_r)|^{n_r} \cdot |\mathcal{N}(\mathfrak{a}_r)|$. Since each element of $\mathbb{M}$ is not unit, $|\mathcal{N}(\mathfrak{x})| \geq 2, \forall \mathfrak{x} \in \mathbb{M}$ and because $\mathcal{N}(\mathfrak{a}_0)$ is finite; our assumption is in direct contradiction with the result.

Now consider $\mathfrak{b}_1^{n_1} \cdot \mathfrak{b}_2^{n_2} \cdot \mathfrak{b}_3^{n_3} \cdot \ldots \cdot \mathfrak{b}_r^{n_r} \cdot \mathfrak{v}_1 = \mathfrak{c}_1^{m_1} \cdot \mathfrak{c}_2^{m_2} \cdot \mathfrak{c}_3^{m_3} \cdot \ldots \cdot \mathfrak{c}_s^{m_s} \cdot \mathfrak{v}_2$. That implies $\mathfrak{b}_1 | (\mathfrak{c}_1^{m_1} \cdot \mathfrak{c}_2^{m_2} \cdot \mathfrak{c}_3^{m_3} \cdot \ldots \cdot \mathfrak{c}_s^{m_s} \cdot \mathfrak{v}_2)$. Since no two $\mathfrak{c}$'s are associates and every element of $\mathbb{M}$ is prime, $\mathfrak{b}_1$ divides one and only one of $\mathfrak{c}$'s say $\mathfrak{b}_1 | \mathfrak{c}_1$. Because $\mathfrak{c}_1$ is prime, there exists a unit element $\mathfrak{u}_1 \in \mathbb{Z}[\alpha]$ such that

$\mathfrak{c}_1 = \mathfrak{u}_1 \cdot \mathfrak{b}_1$. Suppose $m_1 \geq n_1$. Then $\mathfrak{b}_2^{n_2} \cdot \mathfrak{b}_3^{n_3} \cdot \ldots \cdot \mathfrak{b}_r^{n_r} \cdot \mathfrak{v}_1 = \mathfrak{u}_1^{m_1} \cdot \mathfrak{b}_1^{m_1 - n_1} \cdot \mathfrak{c}_2^{m_2} \cdot \mathfrak{c}_3^{m_3} \cdot \ldots \cdot \mathfrak{c}_s^{m_s} \cdot \mathfrak{v}_2 \Rightarrow \mathfrak{b}_1 | (\mathfrak{b}_2^{n_2} \cdot \mathfrak{b}_3^{n_3} \cdot \ldots \cdot \mathfrak{b}_r^{n_r} \cdot \mathfrak{v}_1)$ for $m_1 > n_1$. Because no two $\mathfrak{b}$'s are associates, latter is not possible. Thus, we are left with $m_1 = n_1$. This gives $\mathfrak{b}_2^{n_2} \cdot \mathfrak{b}_3^{n_3} \cdot \ldots \cdot \mathfrak{b}_r^{n_r} \cdot \mathfrak{v}_1 = \mathfrak{u}_1^{m_1} \cdot \mathfrak{c}_2^{m_2} \cdot \mathfrak{c}_3^{m_3} \cdot \ldots \cdot \mathfrak{c}_s^{m_s} \cdot \mathfrak{v}_2$. Continuing this procedure we can see that $r = s$ and after renumbering the $\mathfrak{c}$'s we have $n_i = m_i$, $\mathfrak{b}_i$ is associate of $\mathfrak{c}_i$ for $i = 1, 2, 3, \ldots, r$, and $\mathfrak{v}_1$ is associate of $\mathfrak{v}_2$. □

Definition 2.1 — For $\mathfrak{P}(x) = \mathfrak{a}_n x^n + \mathfrak{a}_{n-1} x^{n-1} + \mathfrak{a}_{n-2} x^{n-2} + \ldots + \mathfrak{a}_0 \in \mathbb{Z}[\alpha][x]$, an element $\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdot \mathfrak{p}_2^{n_2} \cdot \mathfrak{p}_3^{n_3} \cdot \ldots \cdot \mathfrak{p}_r^{n_r} \cdot \mathfrak{u}$ where $\mathfrak{p}_i \in \mathbb{M}$ and $\mathfrak{u}$ is a unit element of $\mathbb{Z}[\alpha]$, is said to be a content of the polynomial $\mathfrak{P}(x)$ if

1. $\mathfrak{a} | \mathfrak{a}_i$, $0 \leq i \leq n$ and
2. If, there exists another element $\mathfrak{b} = \mathfrak{q}_1^{m_1} \cdot \mathfrak{q}_2^{m_2} \cdot \mathfrak{q}_3^{m_3} \cdot \ldots \cdot \mathfrak{q}_s^{m_s} \cdot \mathfrak{v}$, $\forall \mathfrak{q}_j \in \mathbb{M}$ and $\mathfrak{v}$ being a unit element in $\mathbb{Z}[\alpha]$ such that $\mathfrak{b} | \mathfrak{a}_i$ for $0 \leq i \leq n$, then $\mathfrak{b} | \mathfrak{a}$

Furthermore, $\mathfrak{P}(x)$ is called a primitive polynomial over $\mathbb{Z}[\alpha]$ if its content is a unit.

Remark 2.2 : Consider a polynomial $\mathfrak{P}(x) = \mathfrak{a}_n x^n + \mathfrak{a}_{n-1} x^{n-1} + \mathfrak{a}_{n-2} x^{n-2} + \ldots + \mathfrak{a}_0$ over $\mathbb{Z}[\alpha]$. In the light of Theorem 2.1, $\mathfrak{a}_0$ can be factorized in the form $\mathfrak{x}_1^{n_1} \cdot \mathfrak{x}_2^{n_2} \cdot \mathfrak{x}_3^{n_3} \cdot \ldots \cdot \mathfrak{x}_r^{n_r} \cdot \mathfrak{v}$ where $\mathfrak{x}$'s are elements of $\mathbb{M}$ and $\mathfrak{v}$ is a non-zero element of $\mathbb{Z}[\alpha]$ such that $\mathfrak{x} \nmid \mathfrak{v}$, $\forall \mathfrak{x} \in \mathbb{M}$. There exist r non-negative integers $k_1, k_2, k_3, \cdots, k_r$ such that ${\mathfrak{x}_i}^{k_i} | \mathfrak{a}_j$, but, ${\mathfrak{x}_i}^{k_i+1} \nmid \mathfrak{a}_j$ for $0 \leq j \leq n$ and $1 \leq i \leq r$. It is easy to see that $\mathfrak{a} = \mathfrak{x}_1^{k_1} \cdot \mathfrak{x}_2^{k_2} \cdot \mathfrak{x}_3^{k_3} \cdot \ldots \cdot \mathfrak{x}_r^{k_r} \cdot \mathfrak{u}$ is a content of the polynomial $\mathfrak{P}(x)$. Thus, content of any polynomial over $\mathbb{Z}[\alpha]$ exists. Furthermore, a polynomial over $\mathbb{Z}[\alpha]$ can have more than one content and any two of them are associates of each other.

Proposition 2.1 — Consider the set $\mathbb{Q}_0(\alpha) = \{\mathfrak{a} \cdot \mathfrak{b}^{-1} : \mathfrak{a}, \mathfrak{b} \in \mathbb{Z}[\alpha], \mathfrak{b} \neq 0, \mathfrak{x} \nmid \mathfrak{b}, \forall \mathfrak{x} \in \mathbb{M}\}$. $\mathbb{Q}_0(\alpha)$ is a sub-ring of $\mathbb{Q}(\alpha)$. For $|\Psi(m)|$ being a prime number, the function; $\eta : \mathbb{Q}_0(\alpha) \to \mathbb{Z}_{|\Psi(m)|}$, $\eta(\mathfrak{a} \cdot \mathfrak{b}^{-1}) = \theta(\mathfrak{a}) \cdot [\theta(\mathfrak{b})]^{-1}$ where $\mathfrak{a}, \mathfrak{b} \in \mathbb{Z}[\alpha], \mathfrak{b} \neq 0, \mathfrak{x} \nmid \mathfrak{b}, \forall \mathfrak{x} \in \mathbb{M}$; is a ring homomorphism. The function $\theta : \mathbb{Z}[\alpha] \to \mathbb{Z}_{|\Psi(m)|}$ defined as $\theta(\mathfrak{a}) = \mathfrak{a} \bmod (\alpha - m)$ is a ring homomorphism.

The following Lemma will be used to prove the sequel:

Lemma 2.2 — The product of two primitive polynomials over $\mathbb{Z}[\alpha]$ is a primitive polynomial.

PROOF : Let $\mathfrak{F}(x)$ and $\mathfrak{G}(x)$ be two primitive polynomials over $\mathbb{Z}[\alpha]$. Let us assume that $\mathfrak{F}(x) \cdot \mathfrak{G}(x)$ is not primitive. Then $\exists (\alpha - m) \in \mathbb{M}$, such that, $(\alpha - m)$ divides content of $\mathfrak{F}(x) \cdot \mathfrak{G}(x)$. Now, we define a function $\Theta : \mathbb{Z}[\alpha][x] \to \mathbb{Z}_{|\Psi(m)|}[x]$ as $\Theta(\mathfrak{P}(x)) = \theta(\mathfrak{a}_n) x^n + \theta(\mathfrak{a}_{n-1}) x^{n-1} + \theta(\mathfrak{a}_{n-2}) x^{n-2} + \ldots + \theta(\mathfrak{a}_0)$ where $\mathfrak{P}(x) = \mathfrak{a}_n x^n + \mathfrak{a}_{n-1} x^{n-1} + \mathfrak{a}_{n-2} x^{n-2} + \ldots + \mathfrak{a}_0 \in \mathbb{Z}[\alpha][x]$ and the function $\theta : \mathbb{Z}[\alpha] \to \mathbb{Z}_{|\Psi(m)|}$ is defined as $\theta(\mathfrak{a}) = \mathfrak{a} \bmod (\alpha - m)$. Note that function Θ is a

ring homomorphism. Then $\Theta(\mathfrak{F}(x)\cdot\mathfrak{G}(x))=0\Rightarrow\Theta(\mathfrak{F}(x))\cdot\Theta(\mathfrak{G}(x))=0$. Since $\mathbb{Z}_{|\Psi(m)|}[x]$ is an integral domain, either $\Theta(\mathfrak{F}(x))=0$ or $\Theta(\mathfrak{G}(x))=0$. That implies at least one of the considered polynomials is not primitive. □

Lemma 2.3 — If $\mathfrak{F}(x)\in\mathbb{Z}[\alpha][x]$ is reducible over $\mathbb{Q}(\alpha)$ then $\mathfrak{F}(x)$ can be written as a product of two non-constant polynomials in $\mathbb{Q}_0(\alpha)[x]$.

PROOF : Proving the lemma for primitive polynomial is sufficient. Suppose a primitive polynomial $\mathfrak{F}(x)\in\mathbb{Z}[\alpha][x]$ is reduced over $\mathbb{Q}(\alpha)$ as $\mathfrak{F}(x)=\mathfrak{G}(x)\cdot\mathfrak{H}(x)$ where $\mathfrak{G}(x),\mathfrak{H}(x)\in\mathbb{Q}(\alpha)[x]$. Then, there exist $\mathfrak{G}'(x),\mathfrak{H}'(x)\in\mathbb{Z}[\alpha][x]$ and non-zero elements $\mathfrak{a},\mathfrak{b}\in\mathbb{Z}[\alpha]$ such that $\mathfrak{G}(x)=\mathfrak{a}^{-1}\cdot\mathfrak{G}'(x)$ and $\mathfrak{H}(x)=\mathfrak{b}^{-1}\cdot\mathfrak{H}'(x)$. $\mathfrak{c}_1$ and $\mathfrak{c}_2$ are contents of $\mathfrak{G}'(x)$ and $\mathfrak{H}'(x)$ respectively such that $\mathfrak{G}'(x)=\mathfrak{c}_1\cdot\mathfrak{G}_0{}'(x)$ and $\mathfrak{H}'(x)=\mathfrak{c}_2\cdot\mathfrak{H}_0{}'(x)$ where $\mathfrak{G}_0{}'(x)$ and $\mathfrak{H}_0{}'(x)$ are primitive polynomials. Note that $\mathfrak{G}_0{}'(x)$ and $\mathfrak{H}_0{}'(x)$ are non-constant polynomials. That gives us $\mathfrak{v}\cdot\mathfrak{F}(x)=\mathfrak{G}_0{}'(x)\cdot\mathfrak{H}_0{}'(x)$ where $\mathfrak{v}=\mathfrak{a}\cdot\mathfrak{b}\cdot{\mathfrak{c}_1}^{-1}\cdot{\mathfrak{c}_2}^{-1}$. By Lemma 2.2, $\mathfrak{v}\in\mathbb{Z}[\alpha]$ and $\mathfrak{x}\nmid\mathfrak{v}$ for any $\mathfrak{x}\in\mathbb{M}$. Therefore, $\mathfrak{v}^{-1}\mathfrak{G}_0{}'(x)\in\mathbb{Q}_0(\alpha)[x]$. □

We prove the Theorem 1.1 using the Lemma proved above.

3. PROOF OF THEOREM 1.1

PROOF : Suppose $\mathfrak{F}(x)$ is reducible over $\mathbb{Q}(\alpha)$ and $\overline{\mathfrak{F}(x)}$ is irreducible over $\mathbb{Z}_{|\Psi(m)|}$. By lemma 2.3, we can write $\mathfrak{F}(x)=\mathfrak{G}(x)\cdot\mathfrak{H}(x)$ such that $\mathfrak{G}(x)$ and $\mathfrak{H}(x)$ are non-constant polynomials in $\mathbb{Q}_0(\alpha)[x]$. Define a function Ω, from $\mathbb{Q}_0(\alpha)[x]$ into $\mathbb{Z}_{|\Psi(m)|}[x]$, by $\Omega(\mathfrak{P}(x))=\eta(\mathfrak{p}_n)x^n+\eta(\mathfrak{p}_{n-1})x^{n-1}+\eta(\mathfrak{p}_{n-2})x^{n-2}+\ldots+\eta(\mathfrak{p}_0)$ where $\mathfrak{P}(x)=\mathfrak{p}_nx^n+\mathfrak{p}_{n-1}x^{n-1}+\mathfrak{p}_{n-2}x^{n-2}+\ldots+\mathfrak{p}_0\in\mathbb{Q}_0(\alpha)[x]$ and η corresponding to given m is constructed using Proposition 2.1. Note that $\Omega(\mathfrak{F}(x))=\overline{\mathfrak{F}(x)}$. It can be easily verified that Ω is a ring homomorphism. Thus, $\overline{\mathfrak{F}(x)}=\Omega(\mathfrak{G}(x))\cdot\Omega(\mathfrak{H}(x))$. Since $deg\Omega(\mathfrak{G}(x))<deg\overline{\mathfrak{F}(x)}$ and $deg\Omega(\mathfrak{H}(x))<deg\overline{\mathfrak{F}(x)}$, contrary to the assumption, $\overline{\mathfrak{F}(x)}$ is clearly shown to be reducible over $\mathbb{Z}_{|\Psi(m)|}$. □

The following examples are quick applications of the Theorem 1.1:

Example 3.1 : If $|\Psi(m)|$ is prime for some integer m, then taking Theorem 1.1 into consideration, the polynomial $\mathfrak{P}(x)=x^{|\Psi(m)|}-x-1$ is irreducible over $\mathbb{Q}(\alpha)$. Here $\Psi(x)$ is the minimal polynomial of algebraic integer α.

Example 3.2 : For $\alpha=e^{\frac{3\pi i}{8}}$ and $\beta=\frac{-1+(-3+2(\sqrt{5}-1)e^{\frac{3\pi i}{8}})^{\frac{1}{2}}}{2}$, in the light of Theorem 1.1 (β is a zero of a polynomial of degree four over $\mathbb{Z}[\alpha]$ which is irreducible over $\mathbb{Q}(\alpha)$), the field extension $\mathbb{Q}(\alpha,\beta)$ has degree 32 over $\mathbb{Q}$.

ACKNOWLEDGEMENT

I thank Mr. Rajendra Singh Bhati (IISER Mohali) for his help during the manuscript preparation and submission procedure.

REFERENCES

1. J. Brillhart, M. Filaseta, and A. Odlyzko, On an irreducibility theorem of A. Cohn, *Canadian J. Math.*, **33** (1981), 1055-1059.
2. G. Eisenstein, Über die Irreductibilitäl und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt, *J. Reine Angew. Math.*, **39** (1850), 160-182.
3. D. Hilbert, Ueber die Irreducibilitä ganzer rationaler Functionen mit ganzzahligen Coefficienten, *J. Reine Angew. Math.*, **110** (1892), 104-129.
4. Joseph A. Gallian, *Contemporary abstract algebra*, Seventh Edition, Brooks/Cole, Cengage Learning, USA, (2009).
5. M. R. Murty, Prime numbers and irreducible polynomials, *The American Mathematical Monthly*, **109**(5) (2002), 452-458.
6. Steven H. Weintraub, *Galois theory*, Second Edition, Springer, New York, USA, (2009).