Indian J. Pure Appl. Math., **44**(2): 203-230, April 2013
© Indian National Science Academy

REPRESENTATION OF CYCLOTOMIC FIELDS AND THEIR SUBFIELDS[1]

A. Satyanarayana Reddy*, Shashank K. Mehta**,[1] and Arbind K Lal***,[2]

**Department of Mathematics, Shiv Nadar University,*
Dadri 203 207, *India*
***Department of Computer Science and Engineering,*
Indian Institute of Technology, Kanpur 208 016, *India*
***,Department of Mathematics and Statistics,*
Indian Institute of Technology, Kanpur 208 016, *India*
e-mail: satyanarayana.reddy@snu.edu.in, skmehta@cse.iitk.ac.in,
arlal@iitk.ac.in

(*Received* 28 *February* 2011; *accepted* 21 *January* 2013)

Let $\mathbb{K}$ be a finite extension of a characteristic zero field $\mathbb{F}$. We say that a pair of $n \times n$ matrices (A, B) over $\mathbb{F}$ represents $\mathbb{K}$ if $\mathbb{K} \cong \mathbb{F}[A]/\langle B\rangle$, where $\mathbb{F}[A]$ denotes the subalgebra of $\mathbb{M}_n(\mathbb{F})$ containing A and $\langle B\rangle$ is an ideal in $\mathbb{F}[A]$, generated by B. In particular, A is said to represent the field $\mathbb{K}$ if there exists an irreducible polynomial $q(x) \in \mathbb{F}[x]$ which divides the minimal polynomial of A and $\mathbb{K} \cong \mathbb{F}[A]/\langle q(A)\rangle$.

In this paper, we identify the smallest order circulant matrix representation for any subfield of a cyclotomic field. Furthermore, if p is a prime and $\mathbb{K}$ is

[1]This work was partly supported by Research-I Foundation, IIT-Kanpur, Indian Institute of Technology, Kanpur.

[2]Third author takes this opportunity to thank the Concordia University, Canada, for a visiting position, where the draft version of the paper was completed.

a subfield of the p-th cyclotomic field, then we obtain a zero-one circulant matrix A of size $p \times p$ such that $(A, \mathbf{J})$ represents $\mathbb{K}$, where $\mathbf{J}$ is the matrix with all entries 1. In case, the integer n has at most two distinct prime factors, we find the smallest order $0, 1$-companion matrix that represents the n-th cyclotomic field. We also find bounds on the size of such companion matrices when n has more than two prime factors.

Key words : Circulant matrix; Companion Matrix; Cyclotomic field; Cyclotomic Polynomial; Möbius Function; Ramanujan Sum.

1. Introduction and Preliminaries

In this paper, we will be interested in fields $\mathbb{F}$ that have characteristic 0. Thus, one can assume that $\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathbb{C}$, where $\mathbb{Q}$ is the field of rational numbers and $\mathbb{C}$ is the field of complex numbers. An element $\alpha \in \mathbb{C}$ is said to be algebraic over $\mathbb{F}$, if α is a root of a polynomial $f(x) \in \mathbb{F}[x]$. The polynomial $f(x)$ is said to be the minimal polynomial of α over $\mathbb{F}$, if α is a root of $f(x)$, $f(x)$ is monic and is irreducible in $\mathbb{F}[x]$. In this paper, $\mathbb{M}_n(\mathbb{F})$ will denote the set of all $n \times n$ matrices over $\mathbb{F}$. All vectors are column vectors and they are written in bold face. Also, the vector of all 1's is denoted by $\mathbf{e}$ and $\mathbf{J} = \mathbf{e}\mathbf{e}^t$, where $\mathbf{e}^t$ denotes the transpose of $\mathbf{e}$, is a square matrix with each entry 1. The symbol $\emptyset$ will denote either a vector or a matrix having all entries zero.

Recall that for any $A \in \mathbb{M}_n(\mathbb{F})$, a celebrated result, commonly known as the Cayley-Hamilton Theorem, states that the matrix A satisfies its own characteristic polynomial. That is, if $\varsigma_A(x) = \det(xI - A)$ is the characteristic polynomial of A, then $\varsigma_A(A)$ as an element of $\mathbb{F}[A]$, equals $\emptyset$. Let $S = \{f(x) \in \mathbb{F}[x] | f(A) = \emptyset\}$. Then S is an ideal in $\mathbb{F}[x]$ and $S = \langle p(x) \rangle$, for some monic polynomial $p(x) \in \mathbb{F}[x]$. By definition, $p(x)$ divides $\varsigma_A(x)$ and for any $B \in \mathbb{F}[A]$, there exists a unique polynomial $g(x) \in \mathbb{F}[x]$, with $\deg(g(x)) < \deg(p(x))$ such that $B = g(A)$. The polynomial $p(x)$ is called the minimal polynomial of A and is denoted by $p_A(x)$. We are now ready to state a few results from matrix theory and abstract algebra. For proofs and notations related with these results the reader is advised to refer to

the book Abstract Algebra by Dummit & Foote [5] and Linear Algebra by Hoffman and Kunze [7].

Lemma 1.1 (Hoffman and Kunze, Pages $204, 231$ [7]) — Let A be a square matrix.

1. Then A is diagonalizable if and only if its minimal polynomial is separable.
2. Let A be a matrix with distinct eigenvalues. Then a matrix B commutes with A if and only if B is a polynomial in A.

To state the next result, recall that for a monic polynomial $f(x) = x^n - c_{n-1}x^{n-1} - c_{n-2}x^{n-2} - \cdots - c_1x - c_0 \in \mathbb{F}[x]$, its companion matrix, denoted $\mathbb{C}l(f)$, is defined as

$$\mathbb{C}l(f) = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ c_0 & c_1 & c_2 & \dots & c_{n-2} & c_{n-1} \end{bmatrix}.$$

For example, the $n \times n$ matrix

$$W_n = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \end{bmatrix}$$

is the companion matrix of the polynomial $x^n - 1$. Note that W_n is a $0, 1$-circulant matrix and $x^n - 1$ is its minimal polynomial. It is well known (for example, see Davis[4]) that every circulant matrix is a polynomial in W_n. Due to the above property, the matrix W_n is called the fundamental circulant matrix. The next result also appears in [7].

Lemma 1.2 (Hoffman and Kunze, Page 230 [7]) — Let $\mathbb{C}l(f)$ be the companion matrix of $f(x) = x^n - c_{n-1}x^{n-1} - c_{n-2}x^{n-2} - \cdots - c_1x - c_0 \in \mathbb{F}[x]$. Then

1. $f(x)$ is both the minimal and the characteristic polynomial of $\mathbb{C}l(f)$.
2. all eigenvalues of the companion matrix $\mathbb{C}l(f)$ are distinct if and only if $\mathbb{C}l(f)$ is diagonalizable.

The next result is also well known. The proof can be easily obtained by using basic results in abstract algebra and it also appears in [5].

***Theorem* 1.3** — *Let $p_A(x)$ be the minimal polynomial of $A \in \mathbb{M}_n(\mathbb{F})$.*

1. Let $g(x) \in \mathbb{F}[x]$ and let $h(x) = \gcd(g(x), p_A(x))$. Then $\langle g(A)\rangle = \langle h(A)\rangle$.
2. If $q(x)$ is a non-constant factor of $p_A(x)$ in $\mathbb{F}[x]$ then $\mathbb{F}[A]/\langle q(A)\rangle \cong \mathbb{F}[x]/\langle q(x)\rangle$. In particular, if $q(x)$ is irreducible and $q(\alpha) = 0$ for some $\alpha \in \mathbb{C}$ then $\mathbb{F}[A]/\langle q(A)\rangle \cong \mathbb{F}[x]/\langle q(x)\rangle \cong \mathbb{F}(\alpha)$. That is, $\mathbb{F}[A]/\langle q(A)\rangle$ is a field.

As a corollary of Theorem 1.3, one has the following result. To state the result, recall that a pair of $n \times n$ matrices (A, B) over $\mathbb{F}$ is said to represent an extension field $\mathbb{K}$ if $\mathbb{K} \cong \mathbb{F}[A]/\langle B\rangle$, where $\langle B\rangle$ is an ideal in $\mathbb{F}[A]$ generated by B.

Corollary 1.4 — Let $\alpha \in \mathbb{C}$. Then the matrix pair (A, B) represents $\mathbb{F}(\alpha)$, a field, if and only if α is an eigenvalue of A, $q(x)$ is the minimal polynomial of α over $\mathbb{F}$ and $\langle B\rangle = \langle q(A)\rangle$ in $\mathbb{F}[A]$.

That is, suppose that $q(x)$ is the minimal polynomial of an eigenvalue α of A. Then the matrix pair (A, B) represents an extension $\mathbb{K} = \mathbb{F}(\alpha)$ of $\mathbb{F}$ if and only if $\langle B\rangle = \langle q(A)\rangle$. Hence with an abuse of the language, we may say that the matrix A represent $\mathbb{K}$ to mean that $\mathbb{K} = \mathbb{F}(\alpha)$, whenever α is an eigenvalue of A. Also, it is well known that the choice of α is not unique. Therefore, depending on the choice of α the corresponding matrices that represent $\mathbb{K}$ can vary. This issue becomes significant when we search for a smallest representation (in terms of order).

We are now ready to explain the motivation for our study. Let G be a finite group and let $n \in \mathbb{Z}^+$. A matrix representation of G is a homomorphism from G into $GL_n(\mathbb{F})$, where $GL_n(\mathbb{F})$ is the group of invertible $n \times n$ matrices with entries from $\mathbb{F}$. The representation is called faithful if the image of the homomorphism is

isomorphic to G. A similar question arises whether an extension field of $\mathbb{F}$ has a representation in $\mathbb{M}_n(\mathbb{F})$. For example, let α be an algebraic number over $\mathbb{F}$ with $q(x) \in \mathbb{F}[x]$ as its minimal polynomial. Then, using Lemma 1.2 and Corollary 1.4, we see that $\mathbb{F}(\alpha) \cong \mathbb{F}[\mathbb{C}l(q))]$, where $\mathbb{C}l(q)$ is the companion matrix of $q(x)$. This leads to the following natural questions:

1. does there exist a matrix A in $\mathbb{M}_n(\mathbb{F})$ with some specified properties such that $\mathbb{F}[A] \cong \mathbb{F}(\alpha)$?
2. if it exists, what is the smallest possible positive integer n?

For example, fix a positive integer n and consider ζ_n, a primitive n-th root of unity. Then the polynomial $\Phi_n(x)$ over $\mathbb{Q}$, called the n-th cyclotomic polynomial, is the minimal polynomial of ζ_n and hence is irreducible over $\mathbb{Q}$. In this case, is it possible to find a matrix A which is either circulant over $\mathbb{Q}$ or is a $0,1$-companion matrix of $\Phi_n(x)$ such that $\mathbb{Q}[A] \cong \mathbb{Q}(\zeta_n)$? It can easily be checked that this is true only when $n = 1$ or $n = 2$. For $n > 2$, such a result is not true. To understand this, recall that $x^n - 1 = \prod_{d|n} \Phi_d(x)$, where $\Phi_d(x) \in \mathbb{Z}[x]$ is the minimal polynomial of ζ_d in $\mathbb{Q}[x]$ and for any two integers s, t, the notation $s|t$ means that s divides t. Consequently, from Corollary 1.4, it follows that for each divisor d of n,

$$\mathbb{Q}[W_n]/\langle \Phi_d(W_n) \rangle \cong \mathbb{Q}(\zeta_d). \tag{1}$$

In particular, $\mathbb{Q}[W_n]/\langle \Phi_n(W_n) \rangle \cong \mathbb{Q}(\zeta_n)$. That is, in this case, the pair $(W_n, \Phi_n(W_n))$ represents the field $\mathbb{Q}(\zeta_n)$.

To proceed further, recall that a *directed graph* (in short, digraph) is an ordered pair $X = (V, E)$ that consists of two sets V, the vertex set, and E, the edge set, where V is non-empty and $E \subset V \times V$. If $e = (u, v) \in E$ with $u \neq v$ then the edge e is said to be incident from u to v or u is said to be the initial vertex and v the terminal vertex of e. An edge $e = (u, u)$ is called a loop. A digraph is called a graph if $(u, v) \in E$ whenever $(v, u) \in E$, for any two elements $u, v \in V$. A graph is called simple if it has no loops.

Let $X = (V, E)$ be a graph. Then the degree of a vertex $v \in V$, denoted $d(v)$, is the number of edges incident with it. In case v is a vertex of a digraph X, one

defines in-degree of v, denoted $d^+(v)$, as the number of edges that have v as a terminal vertex and out-degree of v, denoted $d^-(v)$, as the number of edges that have v as an initial vertex. The simple graph X that has an edge for each pair of vertices is called a complete graph, denoted K_n, where n is the number of vertices of X. A graph with no edge is called a null graph. The cycle graph on n vertices, say $u_1, u_2, \ldots, u_n$, denoted C_n, is a simple graph in which $\{u_i, u_j\}$ is an edge if and only if $i - j \equiv \pm 1 \pmod{n}$. A graph on n vertices, say $u_1, u_2, \ldots, u_n$, denoted X_n, is called a path graph, if for each $i, 1 \leq i \leq n-1$, the set $\{u_i, u_{i+1}\}$ is an edge. A graph (digraph) X is said to be k- regular if $d(v) = k$ ($d^+(v) = d^-(v) = k$) for all $v \in V$. Unless specified otherwise, all the graphs in this paper are assumed to be finite and simple.

Let $X = (V, E)$ be a digraph on n vertices. Then the adjacency matrix of X, denoted $A = [a_{ij}]$ is a square matrix of order n, with $a_{ij} = 1$ whenever $(i, j) \in E$ and 0, otherwise. In case X is a graph then it can be easily seen that A is a symmetric matrix.

Now, let A be the adjacency matrix of a connected k-regular graph X on n vertices. Then, it is well known that k is a simple eigenvalue of A. Thus, the minimal polynomial of A is of the form $(x - k)q(x)$ for some $q(x) \in \mathbb{Z}[x]$. Note that k is a simple eigenvalue of A implies that $q(k) \neq 0$ and for any other eigenvalue α of A, $q(\alpha) = 0$. Then with $q(x)$ as defined, we state the following well known result. We present the proof for the sake of completeness.

Lemma 1.5 (Hoffman [7]) — Let X be a connected k-regular graph on n vertices with minimal polynomial $(x - k)q(x) \in \mathbb{Z}[x]$. Then the matrix $\mathbf{J}$ equals $\dfrac{n}{q(k)}q(A)$.

PROOF : As X is a k-regular graph, its adjacency matrix A satisfies $A\mathbf{e} = k\mathbf{e}$ and hence

$$\mathbf{J}A = A\mathbf{J} = k\mathbf{J} \text{ and } q(A)\mathbf{e} = q(k)\mathbf{e}. \tag{2}$$

Also, the eigenvectors of A can be chosen to form an orthonormal basis $\mathcal{B}$ of $\mathbb{R}^n$. Hence $\dfrac{1}{\sqrt{n}}\mathbf{e} \in \mathcal{B}$ and thus, for any vector $\mathbf{x} \in \mathcal{B}, \mathbf{x} \neq \mathbf{e}$, $\mathbf{x}^t\mathbf{e} = 0$.

Therefore, $\mathbf{J}\mathbf{x} = \emptyset$ and using Equation (2), $\mathbf{J}\frac{1}{\sqrt{n}}\mathbf{e} = \frac{n}{\sqrt{n}}\mathbf{e} = \big(\frac{n}{q(k)}q(k)\big)\frac{1}{\sqrt{n}}\mathbf{e} = \frac{n}{q(k)}q(A)\frac{1}{\sqrt{n}}\mathbf{e}$. Also, $q(\lambda) = 0$ for any eigenvalue $\lambda \neq k$ of A implies that $q(A)\mathbf{x} = q(\alpha)\mathbf{x} = \emptyset$. That is, $\frac{n}{q(k)}q(A)\mathbf{x} = \emptyset$.

Thus, the image of two matrices $\mathbf{J}$ and $\frac{n}{q(k)}q(A)$ on a basis of $\mathbb{R}^n$ are same and hence the two matrices are equal. Therefore $\mathbf{J} = \frac{n}{q(k)}q(A)$. □

The next corollary is an immediate consequence of Theorem 1.3 and Lemma 1.5.

Corollary 1.6 — Let A be the adjacency matrix of a connected k-regular graph X on n vertices. Then $\mathbb{F}[A]/\langle\mathbf{J}\rangle \cong \mathbb{F}[x]/\langle q(x)\rangle$.

PROOF : Since $q(x)$ is a factor of the minimal polynomial $(x-k)q(x)$ of A, using Theorem 1.3 and Lemma 1.5, one has $\mathbb{F}[x]/\langle q(x)\rangle \cong \mathbb{F}[A]/\langle q(A)\rangle \cong \mathbb{F}[A]/\left\langle \frac{n}{q(k)}q(A)\right\rangle = \mathbb{F}[A]/\langle\mathbf{J}\rangle$. □

Hoffman and McAndrew [8] extended Lemma 1.5 to digraphs and is stated below. Note that in their paper, regular digraph were referred as strongly regular digraph.

Lemma 1.7 (Hoffman and McAndrew (1965) [8]) — Let A be the adjacency matrix of a digraph X. Then there exists a polynomial $g(x) \in \mathbb{Q}[x]$ such that $\mathbf{J} = g(A)$ if and only if X is strongly connected and regular.

In this paper, we consider those $0,1$-companion matrices which have ζ_n as an eigenvalue and use them to determine the smallest order circulant matrix representation for all subfields of cyclotomic fields and in certain cases determine the smallest order $0,1$-companion matrix representation for cyclotomic fields. We begin with a review of some facts related with the representation of cyclotomic fields and their subfields by circulant matrices in Section 2. The results about representations of p-th cyclotomic field, p a prime, by $0,1$-circulant matrices are given in Section 2.1. In section 3 we present results on the size of the smallest order

$0, 1$-companion matrix representations of cyclotomic fields.

2. Representation of Cyclotomic Fields and their Subfields

We start this section with a result about the irreducible factors of the minimal polynomial of a companion matrix. The proof of this result can be easily obtained using the theory of minimal polynomials and Lemmas 1.1 and 1.2. Hence we omit the proof.

Lemma 2.1 — Let $f(x) \in \mathbb{F}[x]$ be a monic separable polynomial with irreducible factors $q_1(x), q_2(x), \ldots, q_k(x)$ in $\mathbb{F}[x]$. Suppose $A \in \mathbb{M}_n(\mathbb{F})$ commutes with the companion matrix $\mathbb{C}l(f)$.

1. Then $A = g(\mathbb{C}l(f))$ for some $g(x) \in \mathbb{F}[x]$.
2. Let α_i be a root of $q_i(x)$ and let $\chi_{q_i,g}(x)$ be the minimal polynomial of $g(\alpha_i)$ over $\mathbb{F}$. Then the minimal polynomial of A is the maximal square-free factor of $\prod_{i=1}^{k} \chi_{q_i,g}(x)$.

In particular, the number of irreducible factors of the minimal polynomial of $g(A)$ in $\mathbb{F}[x]$ are at most the number of irreducible factors of $f(x)$ in $\mathbb{F}[x]$.

Recall that for a fixed positive integer n, $\deg(\Phi_n(x)) = \varphi(n)$, where $\varphi(n)$ denotes the well known Euler-totient function. The function $\varphi(n)$ also gives the number of integers between 1 and n that are coprime to n. We omit the proof of the next result as it directly follows from Lemma 2.1, Theorem 1.3.2. and the fact that $x^n - 1 = \sum_{d|n} \Phi_d(x)$.

***Theorem* 2.2** — *Fix a positive integer n and let $A = g(W_n)$, for some $g(x) \in \mathbb{Q}[x]$ with $1 \leq \deg(g(x)) \leq n-1$. Also, for each divisor d of n, let $\chi_{\Phi_d,g}(x)$ be the minimal polynomial of $g(\zeta_d)$ over $\mathbb{Q}$. Then*

1. *$p_A(x)$, the minimal polynomial of A, is the maximal square free factor of $\prod_{d|n} \chi_{\Phi_d,g}(x)$ and $\deg(\chi_{\Phi_d,g}(x))$ divides $\deg(\Phi_d(x))$.*

2. *the number of irreducible factors of $p_A(x)$ is at most the number of divisors of n.*

3. $\mathbb{Q}\big(g(\zeta_d)\big) \cong \mathbb{Q}[A]/\langle \chi_{\Phi_d,g}(A)\rangle$.

Furthermore, if n is a prime, say p, then the number of irreducible factors of $p_A(x)$ is exactly two. One of the factors is of degree 1 and the degree of the other factor is a divisor of $\varphi(p) = p - 1$.

PROOF : Proofs of Part 1, 2 and 3 are direct consequence of Lemma 2.1 and Theorem 1.3. For the last statement, note that n is prime and hence it has exactly two factors, namely 1 and n. Hence, using Lemma 2.1, it is sufficient to prove that $p_A(x)$ has at least two irreducible factors.

As $A = g(W_n)$, the eigenvalues of A are $g(\zeta_n^i)$ for $0 \leq i \leq n-1$. Now observe that for $i = 0$, $g(\zeta_n^0) = g(1) \in \mathbb{Q}$ as $g(x) \in \mathbb{Q}[x]$. Therefore, $(x - g(1))$ is an irreducible factor of $p_A(x)$. Also, for some $i, 1 \leq i \leq n-1$, if $g(\zeta_n^i) \neq g(1)$ then the minimal polynomial of $g(\zeta_n^i)$ is another irreducible factor of $p_A(x)$. Hence, $p_A(x)$ has at least two irreducible factors.

Thus, we need to show that $g(\zeta_n^i) = g(1)$ cannot hold true for all $i \in \{1, 2 \ldots, n-1\}$. On the contrary, assume that $g(\zeta_n^i) = g(1)$ for all $i, 1 \leq i \leq n-1$. Define, $h(x) = g(x) - g(1) \in \mathbb{Q}[x]$. Then $h(x)$ has n distinct zeros, $\zeta_n^i,\ 0 \leq i \leq n-1$. This contradicts the definition of $h(x)$ and the assumption that $\deg(g(x)) \leq n-1$ as a polynomial $f(x)$ has at most $\deg(f(x))$ zeros over $\mathbb{C}$. □

Theorem 2.2 establishes that, any field which is represented by an $n \times n$ circulant matrix is a subfield of the d-th cyclotomic field for some d that divides n. It also describes the correspondence between the set of all circulant matrices and the set of all subfields of cyclotomic fields. It can also be concluded that the minimal polynomial of every circulant matrix other than the scalar matrix has at least two irreducible factors. One also concludes the next result and hence the proof is omitted.

Corollary 2.3 — Let A be an $n \times n$ circulant matrix. Then A represents a field

$\mathbb{F}$ over $\mathbb{Q}$ if and only if $\mathbb{F}$ is a subfield of $\mathbb{Q}[\zeta_d]$, for some d dividing n.

The next result gives the smallest positive integer d for which a field $\mathbb{L}$ over $\mathbb{Q}$ (as a subfield of $\mathbb{Q}[\zeta_d]$) is represented by a circulant matrix.

Corollary 2.4 — Let $\mathbb{L}$ be a finite extension of $\mathbb{Q}$. If d is the smallest positive integer such that $\mathbb{L}$ is a subfield of $\mathbb{Q}(\zeta_n)$ then the smallest circulant matrix representation of $\mathbb{L}$ is of order d.

PROOF : Since $\mathbb{L}$ is a subfield of $\mathbb{Q}(\zeta_n)$ there exists $g(x) \in \mathbb{Q}[x]$ such that $\mathbb{L} = \mathbb{Q}\big(g(\zeta_d)\big)$. Thus, by Theorem 2.2.3, $\mathbb{L}$ is represented by $A = g(W_d)$.

Now, assume that there exists a $d' \times d'$ circulant matrix $B = h(W_{d'})$ that represents $\mathbb{L}$, for some $d' < d$. Let $\chi_{\Phi_{d',h}}(x) \in \mathbb{Q}[x]$ be the minimal polynomial of $h(\zeta_{d'})$. Then, using Theorem 2.2.3, one has $\mathbb{L} \cong \mathbb{Q}[B]/\langle \chi_{\Phi_{d',h}}(B)\rangle \cong \mathbb{Q}[h(\zeta_{d'})]$. That is, $\mathbb{L}$ is a subfield of $\mathbb{Q}[\zeta_{d'}]$ as well. This contradicts our hypothesis that d was the smallest positive integer such that $\mathbb{L}$ was a subfield of $\mathbb{Q}[\zeta_n]$. Hence, one has the required result. □

Let n, m and a be positive integers with $n = 2^a m$ and $a \geq 1$. Then, it is known that $\mathbb{Q}[\zeta_m] \cong \mathbb{Q}[\zeta_n]$, whenever m is odd and $a = 1$. Let $n = 2^a \cdot m$ for some odd positive integer m. Then, using Corollaries 2.3 and 2.4, the smallest representation of $\mathbb{Q}[\zeta_n]$ is of order n, whenever $a \neq 1$ and its order is $\frac{n}{2}$, whenever $a = 1$. The following theorem gives a $0,1$-symmetric and circulant matrix representation of order n for the largest subfield of $\mathbb{Q}[\zeta_n]$.

***Theorem* 2.5** — *Let* $\delta_n = \zeta_n + \zeta_n^{-1}$.

1. Then $\mathbb{Q}[\delta_n]$ has a symmetric $0,1$-circulant matrix representation of order n.
2. Let $\mathbb{L}$ be a subfield of $\mathbb{Q}[\delta_n]$. Then there exists a symmetric circulant matrix that represents $\mathbb{L}$.

PROOF : Proof of part 1: Let $\mathbb{K} = \mathbb{Q}[\zeta_n]$. Then $\mathbb{Q}[\delta_n]$ is a subfield of $\mathbb{K}$ and ζ_n is a zero of the polynomial $x^2 - \delta_n x + 1 \in \mathbb{Q}[\delta_n][x]$. So, $[\mathbb{K} : \mathbb{Q}[\delta_n]] = 2$. As $A = W_n + W_n^{-1}$, A is a symmetric, $0,1$-circulant matrix. Also δ_n is an eigenvalue

of $W_n + W_n^{n-1} = W_n + W_n^{-1} = A$. Thus, by Theorem 2.2, A represents $\mathbb{Q}[\delta_n]$. This completes the proof of Part 1.

Proof of part 2: Since $\mathbb{L}$ is a subfield of $\mathbb{Q}[\delta_n]$, there exists a polynomial $g(x) \in \mathbb{Q}[x]$ such that $\mathbb{L} = \mathbb{Q}[g(\delta_n)]$. So $\mathbb{L} = \mathbb{Q}[h(\zeta_n)]$ where $h(x) = g(x+x^{n-1})$. Hence $\mathbb{L}$ can be represented by $h(W_n) = g(W_n + W_n^{n-1}) = g(A)$. Clearly, $h(W_n)$ is a symmetric, circulant matrix. Thus, the required result follows. □

We end this subsection, by a remark that gives an improvement on the order of the matrix A of Theorem 2.5, whenever n is an even integer. It is important to note that the representation given in the next remark, need not be a circulant representation. To do this, one uses a well known result that relates the eigenvalues of a cycle graph with the eigenvalues of a path graph.

Remark 2.6 (Bapat, page 27, [2]) : Let n be an even positive integer and let A denote the adjacency matrix of the cycle C_n. Then the following results are well known:

1. 2 and -2 are eigenvalues of A.
2. Let B_m be the adjacency matrix of the path X_m, on m vertices. Then the set of eigenvalues of $B_{n/2-1}$ and the set of distinct eigenvalues of A, different from 2 and -2, are equal.

Thus, the subfields of $\mathbb{Q}[\delta_n]$ can also be represented by $g(B_{n/2-1})$, for some polynomial $g(x) \in \mathbb{Q}[x]$.

2.1 *Representations of Prime Order*

Let p be a prime and let $\mathbb{K}$ be a subfield of $\mathbb{Q}[\zeta_p]$. Then it is shown in this subsection that there exists a zero-one circulant matrix A of order p such that the pair $(A, \mathbf{J})$ represents $\mathbb{K}$. To do this, we define Cayley graphs/digraphs.

Definition 2.7 — Let G be a group and let S be a non-empty subset of G that does not contain the identity element of G. Then the Cayley digraph/graph associated with the pair (G, S), denoted Cay(G, S), has the set G as its vertex set and for any two vertices $x, y \in G$, (x, y) is an edge if $xy^{-1} \in S$.

Observe that Cay(G, S) is a graph if and only if S is closed with respect to inverse ($S = S^{-1} = \{s^{-1} : s \in S\}$). Also, the graph is k-regular if S has k elements. The set S is called the *connection* set of the graph and it can be easily verified that the graph Cay(G, S) is connected if and only if $G = \langle S \rangle$. We also recall that a digraph is called a circulant digraph if its adjacency matrix is a circulant matrix. The next lemma, due to Biggs, states that every circulant digraph can be obtained as a Cayley digraph.

Lemma 2.8 (Biggs [3]) — Consider $\mathbb{Z}_n$ as a cyclic group of order n. Then every Cayley digraph Cay$(\mathbb{Z}_n, S)$ is a circulant digraph. Conversely, every circulant digraph on n vertices is Cay$(\mathbb{Z}_n, S)$, for some non-empty subset S of $\mathbb{Z}_n$.

We now state a result due to Turner [15] that relates the isomorphism of two circulant graphs of prime order with their eigenvalues.

Lemma 2.9 (Turner [15]) — Let X_1 and X_2 be two circulant graphs of prime order. Then they are isomorphic if and only if they have the same set of eigenvalues. Or equivalently, their connection sets are equivalent.

Before proving a couple of results, we recall the following facts. These facts are not stated in the present form but they can be obtained from the results stated on Pages $554, 577$ of Dummit and Foote [5].

Fact 2.10 (Dummit and Foote, Pages $554, 577$ [5]) — Let p be a prime. Then

1. the polynomial $f(x) = 1 + x + \cdots + x^{p-1}$ is irreducible over $\mathbb{Q}$.
2. the Galois group of $\mathbb{Q}[\zeta_p]$ over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}_p^*$, a cyclic group of order $p - 1$.
3. for each divisor d of $p - 1$, $\mathbb{Z}_p^*$ has a unique subgroup of order d and there exists a unique subfield of $\mathbb{Q}[\zeta_p]$ whose degree of extension over $\mathbb{Q}$ is d.

Lemma 2.11 — Let p be a prime number and let k be any factor of $p - 1$. Then the edge set of $K_p = (\mathbb{Z}_p, E)$, the complete graph on p vertices, can be partitioned into k subsets $E_0, E_1, \ldots, E_{k-1}$ such that the digraphs $X_i = (\mathbb{Z}_p, E_i)$,

for $0 \leq i \leq k-1$, are r-regular circulant digraphs, where $r = \frac{p-1}{k}$. Moreover, the digraphs X_i and X_j, for $0 \leq i < j \leq k-1$, are isomorphic.

PROOF : Let α be a generator of $\mathbb{Z}_p^*$. Then $H = \langle \alpha^k \rangle = \{1, \alpha^k, \ldots, \alpha^{k(r-1)}\}$ is a subgroup of $\mathbb{Z}_p^*$ having r elements and let $H_j = \alpha^j H$, for $j = 0, 1, \ldots, k-1$, be the cosets of H in $\mathbb{Z}_p^*$ with $H_0 = H$. It is important to note that H_j, as a subset of $\mathbb{Z}_p$, generates $\mathbb{Z}_p$, for each $j = 0, 1, \ldots, k-1$. Let us now define a digraph X_j by having $\mathbb{Z}_p$ as its vertex set and any two vertices $x, y \in \mathbb{Z}_p$, (x, y) is an edge in X_j if and only if $y - x \in H_j$. Then it is easy to verify that X_j is an r-regular Cayley digraph, Cay$(\mathbb{Z}_p, H_j)$. Also, observe that if we define $A_j = \sum_{h \in H_j} W_p^h$, for $0 \leq j \leq k-1$, then A_j is a $0,1$-circulant matrix and is the adjacency matrix of X_j.

Since the cosets H_j, for $0 \leq j \leq k-1$, are disjoint, one has obtained k disjoint digraphs that are r-regular and this completes the proof of the first part.

We now need to show that the k digraphs, X_j, for $0 \leq j \leq k-1$, are mutually isomorphic. We will do so by proving that the digraphs X_0 and X_j are isomorphic, for $1 \leq j \leq k-1$.

Let us define a map $\psi : V(X_0) \to V(X_j)$ by $\psi(s) = \alpha^j s$ for each $s \in V(X_0)$. Then it can be easily verified that ψ is one-one and onto. Thus, we just need to show that $\psi\big((x, y)\big)$ is an edge in X_j if and only if (x, y) is an edge in X_0. Or equivalently, we need to show that $\psi(y) - \psi(x) \in H_j$ if and only if $y - x \in H_0 = H$. And this holds true as

$$y - x \in H \Leftrightarrow \alpha^j(y - x) \in H_j \Leftrightarrow (\alpha^j y - \alpha^j x) \in H_j \Leftrightarrow \psi(y) - \psi(x) \in H_j.$$

This completes the proof of the lemma. □

Before coming to the main result of this section, we have the following remark.

Remark 2.12 : Let p be a prime and let the cyclic group $\mathbb{Z}_p^* = \langle \alpha \rangle$ and its cosets $H_j = \alpha^j H$, for $0 \leq j \leq k-1$, be defined as in Lemma 2.11. Then

1. using Fact 2.10.3, the Cayley digraphs, $X_0, X_1, \ldots, X_{k-1}$, constructed in the proof of Lemma 2.11 are unique.

2. for a fixed j, $0 \leq j \leq k$, we observe the following.

   (a) For each $h \in H, hH_j = H_j$. That is, for each $t, 0 \leq t \leq r-1$, $\alpha^{tk}H_j = H_j$. That is, $\alpha^j H = \alpha^{j+tk}H$, for all $t, 0 \leq t \leq r-1$.

   (b) Let ζ_p be a primitive p-th root of unity. Then, for each $t, 0 \leq t \leq r-1$,

$$\sum_{h\in H} \left(\zeta_p^{\alpha^j}\right)^h = \sum_{s\in H_j} \zeta_p^s = \sum_{h\in H} \left(\zeta_p^{\alpha^{j+tk}}\right)^h.$$

We are now ready to state and prove the main result of this section.

***Theorem* 2.13** — *Let p be a prime and let $\mathbb{L}$ be a subfield of $\mathbb{Q}[\zeta_p]$. Then there exists a circulant digraph on p vertices whose adjacency matrix represents $\mathbb{L}$.*

PROOF : Let $r = [\mathbb{L} : \mathbb{Q}]$. Then r divides $p-1 = [\mathbb{Q}[\zeta_p] : \mathbb{Q}]$, as $\mathbb{Q} \subset \mathbb{L} \subset \mathbb{Q}[\zeta_p]$. Let $k = \frac{p-1}{r}$. We now claim the existence of a $0,1$-circulant matrix A of order p whose minimal polynomial has an irreducible factor of degree r.

As k divides $p-1$, Lemma 2.11, gives us a collection, say $X_0, X_1, \ldots, X_{k-1}$, of r-regular circulant digraphs on p vertices that are mutually isomorphic. Let A be the adjacency matrix of X_0. Then, using the definition of X_0, its adjacency matrix $A = \sum_{h\in H} W_p^h$. Thus, A is a circulant matrix and hence diagonalizable. Thus, we just need to find the eigenvalues of A to get the minimal polynomial of A. By definition, the eigenvalues of A are $\lambda_i = \sum_{h\in H} (\zeta_p^i)^h$, for $0 \leq i \leq p-1$. Observe that $|\lambda_i| \leq r$ and $\lambda_i = r$ if and only if $i = 0$. Fix an $i \in \{1, 2, \ldots, p-1\}$. Then, $i \in H_j$, for some coset H_j, $0 \leq j \leq k-1$, of $\mathbb{Z}_p^*$. Therefore, using Remark 2.12.2, we see that $\lambda_{\alpha^j} = \lambda_{\alpha^{j+k}} = \cdots = \lambda_{\alpha^{j+(r-1)k}}$, for each $j \in \{0, 1, 2, \ldots, k-1\}$. That is, for each fixed $j \in \{0, 1, \ldots, k-1\}$ and $s, t \in H_j$, $\lambda_s = \lambda_t$. Thus, A has exactly k distinct eigenvalues other than the eigenvalue r. Also, note that A is a circulant matrix of order p, a prime. Therefore, by Theorem 2.2.2, the minimal polynomial of A factors into two distinct irreducible factors. One of the factor is $x - r$, corresponding to the simple eigenvalue r of A and the other must contain

all the distinct eigenvalues of A, different from r. Hence, the minimal polynomial of A equals $(x-r)\prod_{i=1}^{k}(x-\lambda_i) = (x-k)q(x) \in \mathbb{Q}[x]$.

As $\deg(q(x)) = k$, the $0,1$-circulant matrix A represents a subfield, say $\mathbb{K}$, of $\mathbb{Q}[\zeta_p]$ such that $[\mathbb{K} : \mathbb{Q}[\zeta_p]] = k$. Thus, the proof of the claim is complete.

Now, using Fact 2.10.3, the subfield $\mathbb{K}$ is indeed the subfield $\mathbb{L}$. □

We have seen that if p is a prime then $\mathbb{Q}[\zeta_p]$ has a unique subfield for each divisor d of $p-1$. But all the real subfields of $\mathbb{Q}[\zeta_p]$ are also subfields of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. This observation leads to the last result of this section.

Corollary 2.14 — Let p be a prime number. Then every real subfield of $\mathbb{Q}[\zeta_p]$ has a symmetric $0,1$-circulant matrix representation of order p.

Let p be a prime and consider the digraph X_0 in the proof of Theorem 2.13. Since p is a prime, it can be easily verified that X_0 is a strongly connected regular digraph. Hence, using Lemma 1.7, one immediately obtains the following result and hence the proof is omitted.

Corollary 2.15 — Let $\mathbb{L}$ be a subfield of $\mathbb{Q}[\zeta_p]$. Then there exists a $0,1$-circulant matrix A of order p such that $(A, \mathbf{J})$ represents $\mathbb{L}$.

3. Smallest $0,1$-Companion Matrices Whose Minimal Polynomial is Divisible by $\Phi_n(x)$

In this section, for a fixed positive integer n, our objective is to find a $0,1$-companion matrix of the smallest order that represents $\mathbb{Q}[\zeta_n]$. Let α denote the generic element such that $\mathbb{Q}[\alpha] = \mathbb{Q}[\zeta_n]$. Using Corollary 1.4, this is equivalent to finding the smallest $0,1$-companion matrix whose minimal polynomial is divisible by the minimal polynomial of α. As there are infinitely many choices for α, we restrict ourselves to $\alpha = \zeta_n$. Hence, we search for a polynomial $f(x) \in \mathbb{Z}[x]$ of least degree such that $\Phi_n(x)$ divides $f(x)$ and $\mathbb{C}l(f)$, the companion matrix of $f(x)$, is a matrix with entries 0 and 1. A similar study was made by Filaseta and Schinzel [6]

and Steinberger [13], where they looked at polynomials with integer coefficients that are divisible by $\Phi_n(x)$.

Let $f(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_1x - a_0 \in \mathbb{Z}[x]$. Then $\mathbb{C}l(f)$ is a $0,1$-matrix if and only if for each $i, 0 \leq i \leq n-1,\ a_i \in \{0,1\}$. Since $gcd(x^k, \Phi_n(x)) = 1$ for all $k \geq 1$, without loss of generality, we can assume that $a_0 = 1$. By definition, $\Phi_n(x)$ divides $g(x) = x^n - 1$. Hence $\mathbb{C}l(g)$ is a $0,1$-matrix of order n that represents $\mathbb{Q}[\zeta_n]$. In order to determine whether there exists a matrix of smaller order, we define a set $\mathcal{A}_n$ as

$$\mathcal{A}_n = \{f(x) \in \mathbb{Z}[x] \quad : \quad \Phi_n(x) \mid f(x), f(x) \equiv x^m - a_{m-1}x^{m-1} - \cdots a_1x - 1 \\ m < n, a_i \in \{0,1\} \text{ for } 1 \leq i < m\} \tag{3}$$

and try to find the polynomial of least degree in $\mathcal{A}_n$.

Let $f(x) \in \mathcal{A}_n$. Then $f(x)$ has at least three terms as $m < n$. Hence, $f(1) \neq 0$. Now, let p be a prime. Then $\deg(f(x)) > \deg(\Phi_p(x)) = p - 1$. Thus, $\mathcal{A}_p$ is an empty set. This is stated as our next result.

Lemma 3.1 — Let p be a prime number. Then $\mathcal{A}_p$ is an empty set.

Remark 3.2 : Let p be a prime. Then, starting with the field $\mathbb{Q}[\zeta_p]$, a $0,1$-matrix representing $\mathbb{Q}[\zeta_p]$ of least order is W_p, the companion matrix of $x^p - 1$. But, it can be easily seen that if there exists a $0,1$-matrix $A \in \mathbb{M}_\ell(\mathbb{C})$ representing $\mathbb{Q}[\alpha] \cong \mathbb{Q}[\zeta_p]$ then $\ell \geq p - 1$. Thus, it may be possible to get a $0,1$-matrix $A \in \mathbb{M}_{p-1}(\mathbb{C})$ such that A represents $\mathbb{Q}[\alpha] \cong \mathbb{Q}[\zeta_p]$.

We now state a well known result about cyclotomic polynomials which enables us to consider only square-free positive integers n, where recall that a positive integer n is said to be square free if the decomposition of n into primes does not have any repeated factors.

Lemma 3.3 (Prasolov, Page: 93 [12]) — Let p be a prime number and let n be

a positive integer. Then

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p), & \text{if } p \mid n, \\ \frac{\Phi_n(x^p)}{\Phi_n(x)}, & \text{if } p \nmid n. \end{cases}$$

In particular, if $n = p_1^{a_1} \cdots p_k^{a_k}$ is a prime factorization of n into distinct primes $p_1, p_2, \ldots, p_k$ and if $n_0 = p_1 p_2 \cdots p_k$ then $\Phi_n(x) = \Phi_{n_0}(x^{n/n_0})$.

Steinberger [13] pointed out that the problem of finding polynomials divisible by $\Phi_n(x)$ is equivalent to finding polynomials divisible by $\Phi_{n_0}(x)$, where n_0 is the maximum square-free factor of n. Following is a similar assertion in the current context. We give the proof for the sake of completeness.

Lemma 3.4 — Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ be a factorization of n into distinct primes $p_1, p_2, \ldots, p_k$ and let $n_0 = p_1 p_2 \cdots p_k$. Then

$$\min\{\deg(f(x)) : f(x) \in \mathcal{A}_n\} = \frac{n}{n_0} \min\{\deg(f(x)) : f(x) \in \mathcal{A}_{n_0}\}.$$

PROOF : Let $f(x) \in \mathcal{A}_{n_0}$. Then by Lemma 3.3, $f(x^{n/n_0}) \in \mathcal{A}_n$.

Conversely, suppose $f(x) \in \mathcal{A}_n$. Then $\Phi_n(x)$ divides $f(x)$ and therefore using Gauss lemma on polynomials (see Dummit and Foote, Page 304 [5]) and Lemma 3.3,

$$f(x) = \Phi_n(x) g(x) = \Phi_{n_0}(x^{n/n_0}) g(x) \text{ for some } g(x) \in \mathbb{Z}[x].$$

We now group the terms of $g(x)$ such that $g(x) = \sum_{i=0}^{\frac{n}{n_0}-1} g_i(x^{n/n_0}) x^i$, where $g_i(x^{n/n_0})$ is a polynomial in x^{n/n_0} (collect the terms containing the exponents that are equivalent to $i \pmod{n/n_0}$). Therefore,

$$f(x) = \sum_{i=0}^{\frac{n}{n_0}-1} \Phi_{n_0}(x^{n/n_0}) g_i(x^{n/n_0}) x^i = \sum_{i=0}^{\frac{n}{n_0}-1} f_i(x) x^i \text{ (say).}$$

That is, the polynomials $f_i(x)$, for $0 \le i \le n/n_0 - 1$, are divisible by $\Phi_n(x) = \Phi_{n_0}(x^{n/n_0})$. Let the polynomial $f_j(x) x^j$ contain x^m, the leading term of $f(x)$.

Then $f(x) \in \mathcal{A}_n$ implies that

$$\Phi_{n_0}(x^{n/n_0})g_j(x^{n/n_0})x^j = x^m - x^{r_\ell} - x^{r_{\ell-1}} - \cdots - x^{r_1}, \quad \text{with } j \leq r_1 < r_2 < \cdots < r_\ell.$$

As $\gcd(\Phi_n(x), x^{r_1}) = 1$, the polynomial $h(x) = x^{m-r_1} - x^{r_\ell - r_1} - \cdots - x^{r_2 - r_1} - 1$ is expressible as a polynomial in x^{n/n_0} and is divisible by $\Phi_{n_0}(x^{n/n_0})$. Hence, one obtains a polynomial $h_1(y) = y^{m'} - y^{r'_\ell} - \cdots - y^{r'_2} - 1 \in \mathcal{A}_{n_0}$ such that $h(x) = h_1(x^{n/n_0})$ and $\frac{n}{n_0}\deg(h_1) \leq \deg(f) = m$. Thus, the desired result follows. □

Remark 3.5 : Lemma 3.4 implies that in order to determine $\min\{\deg(f(x)) : f(x) \in \mathcal{A}_n\}$, it is sufficient to solve the same problem in $\mathcal{A}_{n_0}$, where n_0 equals the product of all the prime factors of n, a square-free positive integer. Henceforth, n will be a square-free positive integer.

Lemma 3.1 together with Lemma 3.4 leads to our next result.

Lemma 3.6 — Let p be a prime and let $n = p^k$ for some $k \in \mathbb{Z}^+$. Then $\mathcal{A}_n$ is an empty set.

Thus, we will be interested only in those positive integers n that has at least two prime factors. In this case, it will be shown (see Corollary 3.11 on Page 223) that the set $\mathcal{A}_n$ in non-empty. To start with, note that

$$\varphi(n) \leq \min\{\deg(f(x)) : \ f(x) \in \mathcal{A}_n\} < n. \tag{4}$$

Using a small observation, we improve the lower-bound in Equation (4) as follows.

Lemma 3.7 — Let n be a positive integer. Then

$$\max\{\varphi(n), \lceil \frac{n}{2} \rceil\} < \min\{\deg(f(x)) : \ f(x) \in \mathcal{A}_n\} < n. \tag{5}$$

PROOF : The lemma is immediate from Equation (4) if we can show that $\deg(f(x)) > \lceil \frac{n}{2} \rceil$. Suppose $f(x) = x^m - x^{k_\ell} - x^{k_{\ell-1}} - \cdots - x^{k_1} - 1 \in \mathcal{A}_n$

with $0 < k_1 < k_2 < \cdots < k_\ell < m$. As $\Phi_n(x)$ divides $f(x)$, $f(\zeta_n) = 0$. Now, let if possible, $m \leq \frac{n}{2}$. Then $n - 2m \geq 0$ and using the fact that $\zeta_n = \zeta_{2n}^2 = \cos(2\pi/n) + i\sin(2\pi/n)$ and $\zeta_{2n}^n = -1$, we get

$$\begin{aligned} 0 = f(\zeta_n) &= -\zeta_n^m + \zeta_n^{k_\ell} + \zeta_n^{k_{\ell-1}} + \cdots + \zeta_n^{k_1} + 1 \\ &= -\zeta_{2n}^{2m} + \zeta_{2n}^{2k_\ell} + \zeta_{2n}^{2k_{\ell-1}} + \cdots + \zeta_{2n}^{2k_1} + 1 \\ &= 1 + \zeta_{2n}^{n-2m+2k_\ell} + \zeta_{2n}^{n-2m+2k_{\ell-1}} + \cdots + \zeta_{2n}^{n-2m+2k_1} + \zeta_{2n}^{n-2m} \\ &= 1 + \sum_{j=0}^{\ell} \left(\cos\left(\frac{(n-2m+2k_j)\pi}{n} \right) + i \sin\left(\frac{(n-2m+2k_j)\pi}{n} \right) \right), \end{aligned}$$

where $k_0 = 0$. Now using the choice of k_j's, one gets $n - 2m + 2k_j < n$ for each $j = 0, 1, 2, \ldots, \ell$. Hence, $\sum_{j=0}^{\ell} \sin(\frac{(n-2m+2k_j)\pi}{n})$ cannot be zero. Thus, we have arrived at a contradiction and therefore the required result follows. □

This section is arranged as follows: the first subsection is devoted to characterizing $\mathcal{A}_n$ in terms of certain subsets of roots of unity. In Subsection 3.2, the exact value of $\min\{\deg(f(x)) : f(x) \in \mathcal{A}_n\}$ is obtained, whenever n has exactly two prime factors. The last subsection, namely Subsection 3.3, gives a bound on $\min\{\deg(f(x)) : f(x) \in \mathcal{A}_n\}$, whenever n has 3 or more prime factors.

3.1 *Characterization of $\mathcal{A}_n$ by One-Sums*

For a fixed positive integer n, let $U_n = \{k : 1 \leq k \leq n, \gcd(k, n) = 1\}$ and $R_n = \{\zeta_n^k : \ 0 \leq k \leq n-1\}$. Then $|U_n| = \varphi(n)$, R_n contains all the n-th roots of unity and $\{\zeta_n^k : k \in U_n\}$ contains all the primitive n-th roots of unity. The following result can be found in Apostol [1].

Lemma 3.8 (Apostol [1]) — Let n be a positive integer. Then $\sum_{k \in U_n} \zeta_n^k = \mu(n)$, where

$$\mu(n) = \begin{cases} 0, & \text{if } n \text{ is not square free,} \\ 1, & \text{if } n \text{ has even number of prime factors,} \\ -1, & \text{if } n \text{ has odd number of prime factors.} \end{cases}$$

Fix a positive integer n and let $T \subset R_n$. Let $\sigma(T) = \sum_{\alpha \in T} \alpha$, denote the sum of all the elements of T. In particular, recall that $\sigma(R_n) = 0$. We now define a subset $\mathcal{B}_n$ of R_n by

$$\mathcal{B}_n = \{T \subset R_n \setminus \{1\} : \ \sigma(T) = 1\}. \tag{6}$$

Then the next result gives a bijection between the sets $\mathcal{A}_n$ and $\mathcal{B}_n$. This correspondence is useful in constructing members of $\mathcal{A}_n$.

***Theorem* 3.9** — *Let $\mathcal{A}_n$ and $\mathcal{B}_n$ be defined as above. Then there exists a bijection between $\mathcal{A}_n$ and $\mathcal{B}_n$ such that $x^m - 1 - x^{k_1} - x^{k_2} - \cdots - x^{k_l} \in \mathcal{A}_n$ corresponds to $\{\zeta^{n-m}, \zeta^{n-m+k_1}, \cdots, \zeta^{n-m+k_l}\} \in \mathcal{B}_n$.*

PROOF : Let $f(x) = x^m - 1 - x^{k_1} - x^{k_2} - \cdots - x^{k_\ell} \in \mathcal{A}_n$ with $1 \leq k_1 < k_2 < \cdots < k_\ell < m < n$. As $f(x) \in \mathcal{A}_n$, $f(\zeta_n) = 0$ and hence $\zeta_n^m = 1 + \zeta_n^{k_1} + \zeta_n^{k_2} + \cdots + \zeta_n^{k_\ell}$. Or equivalently, $T = \{\zeta_n^{n-m}, \zeta_n^{n-m+k_1}, \ldots, \zeta_n^{n-m+k_\ell}\} \in \mathcal{B}_n$ as $\sigma(T) = 1$.

Conversely, let $T = \{\zeta_n^{k_0}, \zeta_n^{k_0+k_1}, \zeta_n^{k_0+k_2}, \ldots, \zeta_n^{k_0+k_\ell}\} \in \mathcal{B}_n$, where $1 \leq k_0 < k_0 + k_1 < k_0 + k_2 < \cdots < k_0 + k_\ell < n$. Then $\sum_{i=1}^{\ell} \zeta_n^{k_0+k_i} + \zeta_n^{k_0} = 1$, or equivalently, $\zeta_n^{n-k_0} = 1 + \zeta_n^{k_1} + \cdots + \zeta_n^{k_\ell} = 0$. Thus, $f(x) = x^{n-k_0} - x^{k_\ell} - x^{k_{\ell-1}} \cdots - x^{k_1} - 1 \in \mathcal{A}_n$ and the required result follows. □

Theorem 3.9 leads to the following important remark.

Remark 3.10 : Fix a positive integer n and let $f(x)$ be a polynomial of least degree in $\mathcal{A}_n$. Then $\deg(f(x)) = n - k_0$, where k_0 is obtained as follows: "for each element T of $\mathcal{B}_n$, let k_T be the least positive integer such that $\zeta_n^{k_T} \in T$. Then $k_0 = \max\{k_T : T \in \mathcal{B}_n\}$".

We now observe the following. Let n be a positive integer and let d be the product of an even number of distinct prime divisors of n. Also, let us write $\zeta_n^{n/d} = \zeta_d$. Then using Lemma 3.8, $\{\zeta_d^k : \ k \in U_d\} \in \mathcal{B}_n$. Observe that $U_d = \{1, 1 + k_1, 1 + k_2, \ldots, 1 + k_\ell = d - 1\}$ for some k_i's satisfying $1 \leq k_1 < k_2 < \cdots < k_\ell = d - 2$. Therefore, $\zeta_d^{d-1} = \zeta_d^{-1} = 1 + \zeta_d^{k_1} + \cdots + \zeta_d^{k_{l-1}} + \zeta_d^{d-2}$ and hence

$$f(x) = x^{\frac{n}{d}(d-1)} - x^{\frac{n}{d}(d-2)} - x^{\frac{n}{d}(k_{\ell-1})} - \cdots - x^{\frac{n}{d}(k_1)} - 1 \in \mathcal{A}_n$$

is the corresponding polynomial. Note that $\deg(f(x)) = n - \frac{n}{d}$. This observation leads to the first part of the following result. The second part directly follows from the first part and hence the proof is omitted.

Corollary 3.11 — Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ be a factorization of n into distinct primes and let d be the product of an even number of distinct prime divisors of n. If $U_d = \{1, 1 + k_1, 1 + k_2, \ldots, 1 + k_\ell\}$ with $1 \leq k_1 < k_2 < \cdots < k_\ell = d - 2$, then

1. $\Phi_n(x)$ divides the polynomial $f(x) = x^{\frac{n}{d}(d-1)} - x^{\frac{n}{d}(d-2)} - x^{\frac{n}{d}(k_{\ell-1})} - \cdots - x^{\frac{n}{d}(k_1)} - 1$.

2. $\min\{\deg(f(x)) : \ f(x) \in \mathcal{A}_n\} \leq n - \dfrac{n}{p_1 p_2}$, where p_1 and p_2 are the two smallest prime divisors of n.

3.2 *Integers with Two Prime Factors*

Let $n = p_1^{a_1} p_2^{a_2}$ be the factorization of n as product of two distinct primes p_1 and p_2. Then it is shown that the upper bound obtained in Corollary 3.11 is indeed attained. That is, $\min\{\deg(f(x)) : f(x) \in \mathcal{A}_n\} = \frac{n}{p_1 p_2}\{p_1 p_2 - 1\}$.

Before proceeding further, recall that for any positive integer n and non-negative integer m, the Ramanujan's sum is defined as $c_n(m) = \sum_{k \in U_n} (\zeta_n^k)^m$. The next lemma is a well known result related with the Ramanujan's sum (for results related with Ramanujan's sum and coefficients of cyclotomic polynomials, see Moree and Hommerson [11]).

Lemma 3.12 (Moree and Hommerson [11]) — Fix positive integers m and n. Then, for each divisor d of n, $c_n(d) = \mu(\frac{n}{d}) \frac{\varphi(n)}{\varphi(\frac{n}{d})}$. Furthermore, $c_n(m) = c_n(d)$ whenever $\gcd(m, n) = d$.

Let $m < n$ be a positive integer. Then Ramanujan's sum is used to assign a number to a polynomial $g(x) = \sum_{i=0}^{m} a_i x^i \in \mathbb{Q}[x]$ via the sum $\sum_{k \in U_n} g(\zeta_n^k)$,

denoted S_g. Then

$$S_g = \sum_{i=0}^{m} a_i c_n(i) = a_0\varphi(n) + \sum_{d|n} \left(\sum_{i \in U_d} a_{ni/d} \right) \mu(d) \frac{\varphi(n)}{\varphi(d)}. \tag{7}$$

Since, $\Phi_n(x)$ divides $f(x)$, $f(\zeta_n^k) = 0$ for each $k \in U_n$. Thus, the next result is immediate and hence the proof is omitted.

Lemma 3.13 — Let n be a positive integer. Then for each $f(x) \in \mathcal{A}_n$, $S_f = 0$.

Therefore, for any $f(x) \in \mathbb{Q}[x]$, $S_f = 0$ gives a necessary condition for $\Phi_n(x)$ to divide $f(x)$. The next result is the main result of this subsection and it is shown that $\min\{\deg(f(x)) : f(x) \in \mathcal{A}_{p_1p_2}\} = p_1p_2 - 1$, whenever p_1 and p_2 are distinct primes. This result together with Lemma 3.4 implies that if p_1 and p_2 are distinct primes and $n = p_1^{a_1}p_2^{a_2}$, for some positive integers a_1 and a_2, then $\min\{\deg(f(x)) : f(x) \in \mathcal{A}_n\} = \frac{n}{p_1p_2}\{p_1p_2 - 1\}$.

***Theorem* 3.14** *Let p_1 and p_2 be two distinct primes. Then*

$$\min\{\deg(f(x)) : f(x) \in \mathcal{A}_{p_1p_2}\} = p_1p_2 - 1.$$

PROOF : Let $n = p_1p_2$. Then using a contrapositive argument, we will first show that $\min\{\deg(f(x)) : f(x) \in \mathcal{A}_n\} \geq n - 1$. Let $f(x) \in \mathcal{A}_n$ be the polynomial of least degree with $\deg(f(x)) < n - 1$. Then Theorem 3.9 gives the existence of a subset $T = \{\zeta_n^{k_1}, \zeta_n^{k_2}, \ldots, \zeta_n^{k_\ell}\}$ of $\mathcal{B}_n$ with $2 \leq k_1 < k_2 < \cdots < k_\ell$ that corresponds to $f(x)$. Define $g(x) = \sum_{i=1}^{\ell} x^{k_i} - 1$. Then $g(x) \in \mathbb{Z}[x]$ and $g(\zeta_n) = 0$. Thus, for all $k \in U_n, g(\zeta_n^k) = 0$ and $S_g = 0$.

Now, for each divisor d of n, define $N_d = \{i\frac{n}{d} : i \in U_d\} \cap \{k_1, k_2, \ldots, k_\ell\}$. Then, using Equation (7), one has $0 = S_g = \sum_{d|n} |N_d| \ \mu(d) \ \frac{\varphi(n)}{\varphi(d)} - \varphi(n)$. Or equivalently, $\varphi(n) = \sum_{d|n} |N_d| \ \mu(d) \ \frac{\varphi(n)}{\varphi(d)}$. Therefore, using $\mu(p_i) = -1$ for $i = 1, 2$ and $\mu(p_1p_2) = 1$, one gets

$$\frac{|N_n|}{\varphi(n)} = 1 + \frac{|N_{p_1}|}{\varphi(p_1)} + \frac{|N_{p_2}|}{\varphi(p_2)}$$

as $|N_1| = 0$. But observe that $|N_n| < \varphi(n)$ as $k_1 \geq 2$. That is, the left hand side of the above identity is less than 1 which contradicts the expression that appears on the right hand side. Thus, our assumption is not valid and hence $\min\{\deg(f(x)) : f(x) \in \mathcal{A}_n\} \geq n-1$.

As $n = p_1p_2$, Corollary 3.11.2 implies that $\mathcal{A}_n$ is non-empty and hence $\min\{\deg(f(x)) : f(x) \in \mathcal{A}_n\} \leq n-1$. Thus, the required result follows. □

3.3 *Even Integers with* 3 *or more Prime Factors*

In this subsection, we improve the bound given in Corollary 3.11 for all even positive integers that have more than 2 prime factors.

***Theorem* 3.15** *Let $p_1 < p_2 < \cdots < p_k$ be odd primes and let $n = 2p_1p_2\cdots p_k$. Then $\min\{\deg(f(x)) : f(x) \in \mathcal{A}_n\} \leq n - v$ where*

$$v = \begin{cases} \frac{n}{2} \cdot \frac{p_1+p_2}{p_1p_2}, & \text{if } 2p_1 > p_2, \\ \frac{3n}{2p_2}, & \text{if } 2p_1 < p_2 < 3p_1, \\ \frac{n}{2p_1}, & \text{if } 3p_1 < p_2. \end{cases}$$

PROOF : Let $f_0(x)$ be the polynomial of least degree in $\mathcal{A}_n$. We will find numbers v_1 and v_2, as lower bounds for $n-\deg(f_0(x))$ and take $v = max\{v_1, v_2\}$. The value of $v_1 = \frac{n}{2p_1}$ is a direct application of Corollary 3.11 as 2 and p_1 are the smallest two prime divisors of n. Now, let us compute v_2.

To get the value of v_2, consider $T = \{\zeta_n^{nr/2p_1} : r \in U_{2p_1}\} \cup \{\zeta_n^{n\ell/p_2} : \ell \in U_{p_2}\}$. Then using Lemma 3.8, $\sum_{z\in T} z = \sum_{r\in U_{2p_1}} \zeta_n^{nr/2p_1} + \sum_{\ell\in U_{p_2}} \zeta_n^{n\ell/p_2} = 1+(-1) = 0$. Multiplying both sides by $\zeta_n^{n/2p_2}$ and observing that $\left(\zeta_n^{n/2p_2}\right)^{p_2} = -1$ (as p_2 is an odd prime), one gets

$$\begin{aligned} 0 &= \sum_{r\in U_{2p_1}} \zeta_n^{nr/(2p_1)+n/(2p_2)} + \sum_{\ell\in U_{p_2}} \zeta_n^{n\ell/p_2+n/(2p_2)} \\ &= \sum_{r\in U_{2p_1}} \zeta_n^{nr/(2p_1)+n/(2p_2)} + \sum_{\ell\in U_{p_2}, 2\ell<p_2-1} \zeta_n^{n\ell/p_2+n/(2p_2)} + \zeta_n^{\frac{n}{2}} \end{aligned}$$

$$
\begin{aligned}
&+ \sum_{\ell \in U_{p_2}, 2\ell > p_2 - 1} \zeta_n^{n\ell/p_2 + n/(2p_2)} \\
= &\sum_{r \in U_{2p_1}} \zeta_n^{nr/(2p_1) + n/(2p_2)} + \sum_{\ell \in U_{p_2}, 2\ell < p_2 - 1} \zeta_n^{n\ell/p_2 + n/(2p_2)} - 1 \\
&+ \sum_{\ell \in U_{p_2}, 2\ell > p_2 - 1} \zeta_n^{n\ell/p_2 + n/(2p_2)}. \qquad (8)
\end{aligned}
$$

Thus, Equation (8) implies

$$
\begin{aligned}
T' &= \{\zeta_n^{nr/(2p_1)+n/(2p_2)} : r \in U_{2p_1}\} \cup \\
&\quad \{\zeta_n^{n\ell/p_2+n/(2p_2)} : \ell \in U_{p_2} \setminus \{(p_2-1)/2\}\} \in \mathcal{B}_n.
\end{aligned}
$$

That is, $v_2 = \min\{r : \zeta_n^r \in T'\} = \begin{cases} \frac{n}{2}\left(\frac{p_1+p_2}{p_1p_2}\right), & \text{if } 2p_1 > p_2, \\ \frac{3n}{2p_2}, & \text{if } 2p_1 < p_2. \end{cases}$

Hence, using Remark 3.10 the required result follows. □

3.4 *When n is Even and $\Phi_n(x)$ is Flat*

In this subsection, the upper bound for $\min\{\deg(f(x)) : f(x) \in \mathcal{A}_n\}$ is improved further whenever n is even and the cyclotomic polynomial $\Phi_n(x)$ is flat. To do so, recall that the height of a polynomial in $\mathbb{Z}[x]$ is the largest absolute value of its coefficients and a polynomial is said to be flat if its height is 1. Let $A(n)$ be the height of $\Phi_n(x)$. It is known that for all $n < 105$, $\Phi_n(x)$ is flat and height of $\Phi_{105}(x)$ is 2. In fact, the height of $\Phi_n(x)$ is unbounded, see Emma Lehmer [10].

Fix a positive integer k and let $n = 2p_1p_2\cdots p_k$, for distinct odd primes $p_1 < p_2 < \cdots < p_k$. Let $\Phi_n(x) = \prod_{i=1}^{\varphi(n)} (x - x_i) = \sum_{t=0}^{\varphi(n)} (-1)^t e_t x^{\varphi(n)-t}$, where $x_1, x_2, \ldots, x_{\varphi(n)}$ are distinct roots of $\Phi_n(x)$ and $e_t = \sum_{1 \le i_1 < i_2 < \cdots < i_t \le \varphi(n)} \prod_{j=1}^{t} x_{i_j}$. Then it is known that $e_t = e_{\varphi(n)-t}$, for $0 \le t \le \varphi(n)$ and $e_0 = 1$ (see Thangadurai [14]). Further, by Newton-Girard formulas

$$
\begin{aligned}
me_m &= e_{m-1}c_n(1) - e_{m-2}c_n(2) + \ldots \\
&\quad + (-1)^m e_1 c_n(m-1) + (-1)^{m-1} c_n(m). \qquad (9)
\end{aligned}
$$

where $c_n(m)$ is the Ramanujan's sum defined in Page 223. In particular, using Lemma 3.8 $e_1 = c_n(1) = \mu(n) = -1$.

Now let k be an even integer. That is, n is product of odd number of distinct primes. Then for any positive integer $m < p_1$,

$$c_n(m) = \begin{cases} -1, & \text{if } m \text{ is odd,} \\ 1, & \text{if } m \text{ is even.} \end{cases}$$

Now, using Equation (9) recursively, it is easy to show that $e_2 = \cdots = e_{p_1-1} = 0$ and $e_{p_1} = 1$.

With these observations, we have

$$\Phi_n(x) = \begin{cases} x^{\varphi(n)} - x^{\varphi(n)-1} \pm \cdots - x + 1, & \text{if } k \text{ is odd,} \\ x^{\varphi(n)} + x^{\varphi(n)-1} - x^{\varphi(n)-p_1} \pm \cdots - x^{p_1} + x + 1, & \text{if } k \text{ is even.} \end{cases} \tag{10}$$

From now on, we consider only flat cyclotomic polynomials. Then $\Phi_n(x) = f_1(x) - f_2(x)$, for some $0,1$-polynomials $f_1(x)$ and $f_2(x)$. Observe that the representation of $\Phi_n(x)$ as difference of two $0,1$-polynomials is unique. Also, $\Phi_n(\zeta_n) = 0$ implies that $f_1(\zeta_n) - f_2(\zeta_n) = 0$ and hence $f_1(\zeta_n) + \zeta_n^{n/2} \cdot f_2(\zeta_n) = 0$. That is, $\Phi_n(x)$ divides $f_1(x) + x^{n/2} f_2(x)$.

Let $\Phi_n^T(x) = f_1(x) + x^{n/2} f_2(x)$. Then $\Phi_n^T(x)$ is a $0,1$-polynomial and $\Phi_n^T(\zeta_n) = 0$. And from Equation (10), we have

$$\deg(\Phi_n^T(x)) = \begin{cases} \phi(n) - 1 + \frac{n}{2}, & \text{whenever } k \text{ is odd,} \\ \phi(n) - p_1 + \frac{n}{2}, & \text{whenever } k \text{ is even.} \end{cases} \tag{11}$$

We now construct a polynomial $\Phi_n^*(x) \in \mathcal{A}_n$ from $\Phi_n^T(x)$ as follows. Let the degree of $\Phi_n^T(x)$ be D. Consider the monomials in $\Phi_n^T(x)$ having exponent strictly between $D - n/2$ and $n/2$. If x^b is the monomial with smallest exponent among these, then $\Phi_n^*(x) = x^{b+n/2} + x^b - \Phi_n^T(x)$. Since n is even, $\Phi_n(x)$ divides $x^{n/2} + 1$

and hence $\Phi_n(x)^* \in \mathcal{A}_n$. Also, the monomial x^b comes from the polynomial $f_1(x)$ and therefore

$$\deg(\Phi_n^*(x)) = \begin{cases} \frac{n}{2} + \varphi(n), & \text{if } k \text{ is odd,} \\ \frac{n}{2} + \varphi(n) - 1, & \text{if } k \text{ is even.} \end{cases} \tag{12}$$

Since $\Phi_n^*(x) \in \mathcal{A}_n$, using Equation (12), the following result follows and hence the proof is omitted.

Lemma 3.16 — Let $n = 2p_1p_2 \cdots p_k$ be the factorization of n into odd primes $p_1 < p_2 < \cdots < p_k$. Suppose that the cyclotomic polynomial $\Phi_n(x)$ is flat. Then

$$\min\{\deg(f(x)) : f(x) \in \mathcal{A}_n\} \leq \begin{cases} \frac{n}{2} + \varphi(n), & \text{if } k \text{ is odd,} \\ \frac{n}{2} + \varphi(n) - 1, & \text{if } k \text{ is even.} \end{cases}$$

Remark 3.17 : In general, we are not able to give exact comparison between the bounds obtained in Theorem 3.15 and the bound in Lemma 3.16. But it can be checked that whenever $3p_1 < p_2$ then the bound in Lemma 3.16 is better than the bound in Theorem 3.15.

CONCLUSION

In this paper, we have tried to study the representations of subfields of a cyclotomic field with the help of circulant and $0, 1$-companion matrices. In particular, the following results have been obtained.

1. A subfield of a cyclotomic field is representable by some circulant matrix and conversely every circulant matrix represents a subfield of a cyclotomic field.

2. Every real subfield of $\mathbb{Q}[\zeta_n]$ is representable by a polynomial in the adjacency matrix of C_n, the cyclic graph. Consequently, every real subfield of $\mathbb{Q}[\zeta_n]$ has integer symmetric circulant matrix representation.

3. Let p be a prime and let $\mathbb{K}$ be a subfield $\mathbb{Q}[\zeta_p]$. Then a $0,1$ circulant matrix A of order p is obtained such that $(A, \mathbf{J})$ represents $\mathbb{K}$.

4. Let $n = p^k$ for some prime p. Then the smallest $0,1$-companion matrix having ζ_n as an eigenvalue is W_n, the companion matrix of $x^n - 1$.

5. Let $n = p_1^{a_1} p_2^{a_2}$ be the prime factorization of n as product of distinct primes. Then $\min\{\deg(f(x)) : f(x) \in \mathcal{A}_n\} = \frac{n}{p_1 p_2}(p_1 p_2 - 1)$.

6. Let n be a positive integer having 3 or more prime factors. Then $\min\{\deg(f(x)) : f(x) \in \mathcal{A}_n\} \leq \frac{n}{p_1 p_2}(p_1 p_2 - 1)$, where p_1 and p_2 are the smallest two distinct primes dividing n. Furthermore, if n is even then this upper bound is improved in Theorem 3.15 and Lemma 3.16.

   It will be nice to improve the bounds obtained in this paper. Also, it will be nice to get examples where the bounds are attained.

REFERENCES

1. Tom M. Apostol, *Introduction to Analytic Number theory*, Springer-Verlag, New York (1976).

2. R. B. Bapat, *Graphs and Matrices*, Springer (2010).

3. N. L. Biggs, *Algebraic Graph Theory* (second edition), Cambridge University Press, Cambridge (1993).

4. Philip J. Davis, *Circulant matrices*, A Wiley-Interscience publications (1979).

5. David S. Dummit and Richard M. Foote, *Abstract Algebra* (second edition), John Wiley and Sons (2002).

6. Michael Filaseta and Andrzej Schinzel, On Testing the Divisibility of Lacunary Polynomials by Cyclotomic Polynomials, *Mathematics of Computation*, **73**(246) (2004), 957-965.

7. A. J. Hoffman, On the polynomial of a graph, *The American Mathematical Monthly*, **70**(1) (1963), 30-36.

8. A. J. Hoffman and M. H. McAndrew, The Polynomial of a Directed Graph, *Proceedings of the American Mathematical Society*, **16**(2) (1965), 303-309.

9. Kenneth Hoffman and Ray Kunze, *Linear Algebra* (second edition), Prentice-Hall (1971).

10. Emma Lehmer, On the magnitude of the coefficients of the cyclotomic polynomial, *Bull. Amer. Math. Soc*., **42** (1936), 389-392.

11. Pieter Moree and Huib Hommerson, *Value distribution of Ramanujan sums and of cyclotomic polynomial coefficients*, arXiv:math/0307352v1 [math.NT] 27 Jul (2003).

12. Victor V. Prasolov, *Polynomials*, Springer (2001).

13. John P. Steinberger, Minimal Vanishing Sums of Roots of Unity with Large Coefficients, *Proc. London Math. Soc*., **97**(3) (2008), 689-717.

14. R. Thangadurai, *On the coefficients of cyclotomic polynomials*, Proceedings of the Summer school on Cyclotomic Fields, June, 1999, Bhaskaracharya Pratishthana, Pune, 311-322, MR1802391 (2001k:11213) (2000).

15. James Turner, Point-symmetric graphs with a prime number of points, *J. Combinatorial theory*, **3** (1967), 136-145.