A note on circulant matrices of degree l^2

DUBOVSKÝ Viktor

VŠB-TU Ostrava, 17. listopadu 15/2172, 708 33 Ostrava-Poruba, CZ
E-mail: viktor.dubovsky@vsb.cz

Abstract: Circulant matrices have quite wide range of application in many different branches of mathematics, such as data and time-series analysis, signal procesing or Fourier transformation. Huge number of results concerning circulant matrices could be found in algebraic number theory, this is because from the ring of circulant matrices of prime degree p one could construct factor ring isomorphic to the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$. In this paper connection between ring of circulant matrices of degree l^2, ie. C_{l^2}, with l equal to odd prime, and the l^2-th cyclotomic field is discused/shown.

Keywords: circulant matrix, cyclotomic field

1 Introduction

A square matrix of degree n is called *circulant matrix* if its each row is cyclic shift of the row above, i.e. it is the matrix of the form

$$\mathbf{A} = \begin{pmatrix} a_0 & a_1 & a_2 & & & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & a_2 & & \cdots & a_{n-2} \\ & a_{n-1} & a_0 & a_1 & \ddots & & \vdots \\ \vdots & & \ddots & a_0 & \ddots & & \\ & & & \ddots & \ddots & & a_2 \\ & & & & & & a_1 \\ a_1 & \cdots & & & & a_{n-1} & a_0 \end{pmatrix}.$$

The entry a_{jk} on j-th row and k-th column, can be computed from the first row element a_i with $a_i \equiv k - j \pmod{n}$. This means that the circulant matrix is fully determined by its first row and so is often denoted by $\mathbf{A} = circ_n(a_0, a_1, \ldots, a_{n-1})$, and this notation will be used in this paper.

The sum and product of two circulant matrices is also circulant and hence the set of all circulant matrices of degree n forms a ring, denoted by $\mathcal{C}_n$.

Another useful and well known fact is that circulant matrices are diagonalizable using the *Fourier matrix* $\mathbf{F}_n$, i.e. the matrix with

$$\mathbf{F}_n = \left(\frac{\zeta_n^{ij}}{\sqrt{n}}\right)_{i,j=0,1,\ldots,n-1,} = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & & & \cdots & 1 \\ 1 & \zeta_n & \zeta_n^2 & & & \cdots & \zeta_n^{(n-1)} \\ & \zeta_n^2 & \zeta_n^4 & & \ddots & & \zeta_n^{2(n-1)} \\ \vdots & & \ddots & & \ddots & & \vdots \\ & & & \ddots & \ddots & & \\ & & & & & & a_1 \\ 1 & \cdots & & & & \zeta_n^{(n-2)(n-1)} & \zeta_n^{(n-1)(n-1)} \end{pmatrix},$$

where ζ_n is a primitive root of unity, i.e. $\zeta_n = \mathrm{e}^{\frac{2\pi\mathrm{i}}{n}} = \cos\frac{2\pi\mathrm{i}}{n} + \mathrm{i}\sin\frac{2\pi\mathrm{i}}{n}$.

The diagonal matrix $\mathbf{D} = \mathbf{F}_n\mathbf{A}\mathbf{F}_n^{-1}$ has entries λ_i equal to

$$\lambda_i = a_0 + a_1\zeta_n^i + a_2\zeta_n^{2i} + \cdots + a_{n-1}\zeta_n^{(n-1)i}. \tag{1}$$

From this we see that λ_i can be viewed as element of the n-th cyclotomic field $\mathbb{Q}(\zeta_n)$. Since the Fourier matrix $\mathbf{F}_n$ is unitary, the determinants $|\mathbf{A}|$ and $|\mathbf{D}|$ are equal and λ_i are eigenvalues of circulant matrix $\mathbf{A}$. Thus we can write $|\mathbf{A}| = \prod_{i=0}^{n-1}\lambda_i$, with $\lambda_0 = a_0 + a_1 + \cdots + a_{n-1}$ and λ_i defined by (1) for $i = 1, 2, \ldots, n-1$.

This observations leads to connection between the ring $\mathcal{C}_n$ of all circulant matrices and the field $\mathbb{Q}(\zeta_n)$. With this connection one can try to use circulant matrices to represent the elements and the arithmetics of the field $\mathbb{Q}(\zeta_n)$.

This is straightforward in the case of $n = l$, where l is odd prime, since in this case all eigenvalues λ_i for $i = 1, 2, \ldots, l-1$ are conjugates and

$$\begin{aligned} |\mathbf{A}| = \prod_{i=0}^{l-1}\lambda_i = (a_0 + a_1 + \cdots + a_{n-1})\prod_{i=1}^{l-1}\lambda_i = (a_0 + a_1 + \cdots + a_{n-1})\,\mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\lambda_1) = \\ = (a_0 + a_1 + \cdots + a_{n-1})\,\mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta_n^{(n-1)}\right), \end{aligned}$$

where $\mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\alpha)$ denotes the norm of the element $\alpha \in \mathbb{Q}(\zeta_l)$. For further details see paper [2].

The relation between $\mathcal{C}_n$ and $\mathbb{Q}(\zeta_n)$ where $n = pq$, the product of two different odd primes p, q is described in [3]. The case of $\mathcal{C}_9$ and $\mathbb{Q}(\zeta_9)$ is discussed in [1].

The purpose of this paper is to find a way to represent the field $\mathbb{Q}(\zeta_{l^2})$. Unfortunately for $n = l^2$, the cyclotomic field is not tamely ramified and because of this it does not pose normal integral basis.

2 Basic observations

The degree of the field $\mathbb{Q}(\zeta_{l^2})$ is $[\mathbb{Q}(\zeta_{l^2}) : \mathbb{Q}] = \varphi(l^2) = l(l-1)$, where φ is Euler's totient function[1].

Unfortunatelly, the m-th cyclotomic field $\mathbb{Q}(\zeta_m)$ has a normal basis, i.e. the basis consisting of elements conjugated by the Galois group, if and only if m is squarefree. Surely this is not our case and thus we are bound to work with a power basis.

[1] *Euler's totient function* or *Euler's phi function* $\varphi(n)$ is defined as number of positive integers $\leq n$ that are relatively prime to n, i.e. integers k with $\gcd(k, n) = 1$. Such integers are called the *totatives* of n.

The power basis of $\mathbb{Q}(\zeta_{l^2})$ consists of elements $1, \zeta_{l^2}, \zeta_{l^2}^2, \ldots, \zeta_{l^2}^{l(l-1)-1}$ and hence every element $\gamma \in \mathbb{Q}(\zeta_{l^2})$ can be written in the form $\gamma = c_0 + c_1\zeta_{l^2} + c_2\zeta_{l^2}^2 + \cdots + c_{l(l-1)-1}\zeta_{l^2}^{l(l-1)-1}$.

Let $\mathbf{A}$ be circulant matrix of degree l^2, $\mathbf{A} = circ_{l^2}(a_0, a_1, \ldots, a_{l^2-1})$. Since the eigenvalues of the matrix $\mathbf{A}$ could be viewed as elements of the field $\mathbb{Q}(\zeta_{l^2})$, this relationship leads to the homomorphism between the ring $\mathcal{C}_{l^2}$ and the field $\mathbb{Q}(\zeta_{l^2})$. So define mapping ψ as follows

$$\psi : \mathcal{C}_{l^2} \longrightarrow \mathbb{Q}(\zeta_{l^2}), \quad \psi : \mathbf{A} \longmapsto \sum_{i=0}^{l^2-1} a_i \zeta_{l^2}^i.$$

In order to check that ψ is a homomorphism, we have to prove following equalities

$$\psi(\mathbf{A} + \mathbf{B}) = \psi(\mathbf{A}) + \psi(\mathbf{B}), \text{ and } \psi(\mathbf{A} \cdot \mathbf{B}) = \psi(\mathbf{A}) \cdot \psi(\mathbf{B}),$$

for circulant matrices $\mathbf{A}, \mathbf{B} \in \mathcal{C}_{l^2}$.

The first part is obvious. In second observe that for matrices $\mathbf{A} = circ_{l^2}(a_0, a_1, \ldots, a_{l^2-1})$, $\mathbf{B} = circ_{l^2}(b_0, b_1, \ldots, b_{l^2-1})$ the entries c_k of the product $\mathbf{C} = \mathbf{A} \cdot \mathbf{B} = circ_{l^2}(c_0, c_1, \ldots, c_{l^2-1})$ have form

$$c_k = \sum_{\substack{i+j \equiv k \\ (\mathrm{mod}\ l^2)}} a_i b_j. \tag{2}$$

The product $\gamma = \alpha\beta \in \mathbb{Q}(\zeta_{l^2})$ with elements $\psi(\mathbf{A}) = \alpha = a_0 + a_1\zeta_{l^2} + \cdots + a_{l^2-1}\zeta_{l^2}^{l^2-1}$ and $\psi(\mathbf{B})\beta = b_0 + b_1\zeta_{l^2} + \cdots + b_{l^2-1}\zeta_9^{l^2-1}$ is of the form $\gamma = c_0 + c_1\zeta_{l^2} + \cdots + c_{l^2-1}\zeta_9^{l^2-1}$, with coefficients c_k satisfying the equation (2) again, because here we do not express the elements α, β and γ in power basis and the exponents of ζ_{l^2} are reduced only by relation $\zeta_{l^2}^{l^2} = 1$, i.e. modulo l^2.

The above observations show that ψ is a homomorphism. Surely the image of ψ is entire field $\mathbb{Q}(\zeta_{l^2})$, so ψ is surjective. But the example of the matrices $circ_{l^2}(0, 0, \ldots, 0) \neq circ_{l^2}(1, 1, \ldots, 1)$ with $\psi(circ_{l^2}(0, 0, \ldots, 0)) = 0$ and $\psi(circ_{l^2}(1, 1, \ldots, 1)) = 0$ shows, that ψ is not injective.

In order to express $\psi(\mathbf{A}) \in \mathbb{Q}(\zeta_{l^2})$ with respect to the power basis we have to replace the terms ζ_{l^2} with exponents greater than $l(l-1)$. This is could be done using the cyclotomic polynomial $\Phi_{l^2}(x) = 1 + x^l + x^{(2l)} + \cdots + x^{(l(l-1))}$, the equality $\Phi_{l^2}(\zeta_{l^2}) = 0$, and henceforth $\zeta_{l^2}^{l(l-1)} = \sum_{i=0}^{l-2} \zeta_{l^2}^{il}$. Formally this means use of the isomorphism $\mathbb{Q}(\zeta_{l^2}) \cong \mathbb{Q}[x]/\Phi_{l^2}(x)$.

This means that the image $\psi(\mathbf{A})$ could be written as

$$\psi(circ_{l^2}(a_0, a_1, \ldots, a_{l^2-1})) = a_0 + a_1\zeta_{l^2} + \cdots + a_{l^2-1}\zeta_{l^2-1}^{l^2-1} = \sum_{j=0}^{l-1}\sum_{i=0}^{l-2}(a_{li+j} - a_{l(l-1)+j})\zeta_{l^2}^{li+j}. \tag{3}$$

From equation (3) we can conclude how the kernel of homomorphism ψ looks like. Since for $\mathbf{A} \in \ker(\psi)$ we have $\psi(\mathbf{A}) = 0 \in \mathbb{Q}(\zeta_{l^2})$, the following equalities have to be satisfied

$$a_{li+j} = a_{l(l-1)+j}, \text{ for all } i = 0, 1, \ldots l-2, j = 0, 1, \ldots l-1.$$

This shows that the kernel $\ker(\psi)$ is the set

$$\{circ_{l^2}(x_0, x_1, x_2, \ldots, x_{l-1}, x_0, x_1, x_2, \ldots, x_{l-1}, \ldots, \ldots, x_0, x_1, x_2, \ldots, x_{l-1}) ; x_i \in \mathbb{Q}\}. \tag{4}$$

The kernel $\ker(\psi)$ is an ideal in $\mathcal{C}_{l^2}$, denote it as $\mathcal{I}_{l^2}$, construct a factor ring $\mathcal{C}_{l^2}/\mathcal{I}_{l^2}$. To prove that this factor ring is a field we have to show that the ideal $\mathcal{I}_{l^2}$ is maximal, i.e. if there is an ideal $\mathcal{J}$ such that $\mathcal{I}_{l^2} \subset \mathcal{J} \subset \mathcal{C}_{l^2}$ then $\mathcal{I}_{l^2} = \mathcal{J}$ or $\mathcal{J} = \mathcal{C}_{l^2}$.

So let $\mathbf{A}$ be matrix such that $\mathbf{A} \notin \mathcal{I}_{l^2}$, $\mathcal{J}$ be an ideal generated by the matrix $\mathbf{A}$ and the ideal $\mathcal{I}_{l^2}$. Finally by $\mathbf{A}^{\times}$ denote circulant matrix from ideal $\mathcal{I}_{l^2}$ with entries x_i of the following form

$$x_0 = \frac{1 - \sum_{j=0}^{l-1} a_{lj}}{l}, \text{ for } i = 0, \text{ and } x_i = -\frac{\sum_{j=0}^{l-1} a_{lj+i}}{l}, \text{ for } i = 1, 2, \ldots, l-1.$$

The matrix $\mathbf{J} = \mathbf{A} + \mathbf{A}^{\times}$ is an element of ideal $\mathcal{J}$, but as the investigation of its eigenvalues shows, $\mathbf{J}$ is invertible and thus $\mathcal{J} = \mathcal{C}_{l^2}$. Eigenvalues of circulant matrices, λ_i, are described in (1). Especially λ_0 is the sum of row entries, i.e. for $\mathbf{J}$ we have

$$\lambda_0 = a_0 + a_1 + \cdots + a_{l^2-1} + lx_0 + lx_1 + \cdots + lx_{l-1} = 1.$$

For λ_1 we have

$$\lambda_1 = \sum_{i=0}^{l^2-1} (a_i + x_{i \bmod l})\, \zeta_{l^2}^{i} = \sum_{j=0}^{l-1} \sum_{k=0}^{l-2} (a_{lk+j} - a_{l(l-1)+j}) \zeta_{l^2}^{lk+j}.$$

At least one coefficient of λ_1 is nonzero since $\mathbf{A} \notin \mathcal{J}$ and so we have $\lambda_1 \neq 0$. The same is true for all λ_i with $\gcd(i, l^2) = 1$.

Finally λ_l can be expressed as

$$\lambda_l = \sum_{i=0}^{l^2-1} (a_i + x_{i \bmod l})\, \zeta_{l^2}^{il} = \sum_{j=0}^{l-1} \sum_{k=0}^{l-1} (a_{li+j} + x_j) \zeta_{l^2}^{lj} = \sum_{j=0}^{l-1} \big((\sum_{k=0}^{l-1} a_{kl+j}) - lx_j \big) \zeta_{l^2}^{lj} = 1.$$

Similarly we can show that $\lambda_i = 1$ for all i with $\gcd(i, l^2) = l$.[2]

From the above we conclude that the determinant $|\mathbf{J}|$ is nonzero, and hence $\mathbf{J}^{-1} \in \mathcal{C}_{l^2}$ exists. The matrix $\mathbf{J}$ is element of the ideal $\mathcal{J}$ and so for every $\mathbf{C} \in \mathcal{C}_{l^2}$ the product $\mathbf{C} \cdot \mathbf{J}$ is element of $\mathcal{J}$. Especially $\mathbf{J}^{-1} \cdot \mathbf{J} = \mathbf{I}$, i.e. the identity matrix, is in $\mathcal{J}$. This shows that $\mathcal{J} = \mathcal{C}_{l^2}$ and that $\mathcal{I}_{l^2}$ is maximal ideal and $\mathcal{C}_{l^2}/\mathcal{I}_{l^2}$ is a field.

There is exactly one matrix of the form $circ_{l^2}\left(c_0, c_1, \ldots, c_{l(l-1)-1}, 0, 0, \ldots, 0\right)$ in every class of the field $\mathcal{C}_{l^2}/\mathcal{I}_{l^2}$. Denote the set of all circulant matrices of such form by $\mathcal{C}_{l^2}^{*}$. Clearly $\psi\left(\mathcal{C}_{l^2}^{*}\right) = \mathbb{Q}\left(\zeta_{l^2}\right)$ and for $\mathbf{A}, \mathbf{B} \in \mathcal{C}_{l^2}^{*}$ also $\psi\left(\mathbf{A} + \mathbf{B}\right) = \psi\left(\mathbf{A}\right) + \psi\left(\mathbf{B}\right)$ holds true. But the product $\mathbf{C} = \mathbf{A} \cdot \mathbf{B}$ may not belong to $\mathcal{C}_{l^2}^{*}$. Thus to get the ring structure on the set $\mathcal{C}_{l^2}^{*}$ we have to define multiplication in another way. For this purpose, take $\mathbf{A}, \mathbf{B} \in \mathcal{C}_{l^2}^{*}$ and corresponding elements $\alpha, \beta \in \mathbb{Q}\left(\zeta_{l^2}\right)$ and let the product $\mathbf{A} * \mathbf{B}$ be

$$\begin{aligned}
\mathbf{A} * \mathbf{B} &= circ_{l^2}\left(a_0, a_1, \ldots, a_{l(l-1)-1}, 0, \ldots, 0\right) * circ_{l^2}\left(b_0, b_1, \ldots, b_{l(l-1)-1}, 0, \ldots, 0\right) = \\
&= circ_{l^2}\left(a_0, a_1, \ldots, a_{l(l-1)-1}, 0, \ldots, 0\right) \cdot circ_{l^2}\left(b_0, b_1, \ldots, b_{l(l-1)-1}, 0, \ldots, 0\right) \\
&\qquad - circ_{l^2}\left(c_{l(l-1)}, c_{l(l-1)+1}, \ldots, c_{l^2-1}, \ldots, c_{l(l-1)}, c_{l(l-1)+1}, \ldots, c_{l^2-1}\right) = \\
&= circ_{l^2}\left(c_0 - c_{l(l-1)}, c_1 - c_{l(l-1)+1}, c_2 - c_{l(l-1)+2}, \ldots, c_l - c_{l(l-1)}, \ldots, c_{l(l-1)-1} - c_{l^2-1}, 0, \ldots, 0\right) \in \mathcal{C}_{l^2}^{*},
\end{aligned} \tag{5}$$

with $c_k = \sum_{\substack{i+j \equiv k \\ (\mathrm{mod}\ l^2)}} a_i b_j$ as in (2).

[2]The $\gcd(i, j)$ is the *greatest common divisor* of integers i, j, i.e. the largest positive integer that divides both i and j.

With the help of (2) and (4) we can show

$$\begin{aligned}\psi(\mathbf{A}*\mathbf{B}) &= \psi\left(\mathbf{A}\cdot\mathbf{B} - circ_{l^2}\left(c_{l(l-1)},\ldots,c_{l^2-1},\ldots,c_{l(l-1)},\ldots,c_{l^2-1}\right)\right) = \\ &= \psi(\mathbf{A}\cdot\mathbf{B}) - \psi\left(circ_{l^2}\left(c_{l(l-1)},\ldots,c_{l^2-1},\ldots,c_{l(l-1)},\ldots,c_{l^2-1}\right)\right) = \\ &= \psi(\mathbf{A}\cdot\mathbf{B}) - 0 = \psi(\mathbf{A})\cdot\psi(\mathbf{B}) = \alpha\cdot\beta \in \mathbb{Q}(\zeta_{l^2}),\end{aligned}$$

which means that mapping ψ reduced to $\mathcal{C}^*_{l^2}$ as follows

$$\psi : \mathcal{C}^*_{l^2} \longrightarrow \mathbb{Q}(\zeta_{l^2}), \quad \psi : \mathbf{A} \longmapsto a_0 + a_1\zeta_{l^2} + a_2\zeta_{l^2}^2 + \cdots + a_{l(l-1)-1}\zeta_9^{l(l-1)-1}$$

is homomorphism again. Moreover since the kernel is trivial in this case we have also proved that $\left(\mathcal{C}^*_{l^2},+,*\right) \simeq \mathbb{Q}(\zeta_{l^2})$.

3 Representation of the field $\mathbb{Q}(\zeta_{l^2})$

In the previous section we have derived straightforward way of representation of $\mathbb{Q}(\zeta_{l^2})$ by circulant matrices from $\mathcal{C}^*_{l^2}$. In this section we try to improve this representation, since the determinant of the circulant matrix $\mathbf{C} = circ_{l^2}\left(c_0, c_1, \ldots, c_{l(l-1)}, 0, \ldots, 0\right)$ is not equal to the norm of the corresponding element $\gamma \in \mathbb{Q}(\zeta_{l^2})$, $\mathrm{N}_{\mathbb{Q}(\zeta_{l^2})/\mathbb{Q}}(\gamma)$. Also the trace of $\mathbf{C}$ is not equal to the trace of γ, $\mathrm{Tr}_{\mathbb{Q}(\zeta_{l^2})/\mathbb{Q}}(\gamma)$ and the multiplication in $\mathcal{C}^*_{l^2}$ or work with classes in $\mathcal{C}_{l^2}/\mathcal{I}_{l^2}$ could be quite awkward.

Let $\alpha = a_0 + a_1\zeta_{l^2} + \cdots + a_{l(l-1)-1}\zeta_{l^2}^{l(l-1)-1}$ and $\alpha^{-1} = x_0 + x_1\zeta_{l^2} + \cdots + x_{l(l-1)-1}\zeta_{l^2}^{l(l-1)-1}$ is its inverse and corresponding matrices from $\mathcal{C}^*_{l^2}$ as described above, then from the equality

$$circ_{l^2}\left(a_0, a_1, \ldots, a_{l(l-1)-1}, 0, \ldots, 0\right) * circ_{l^2}\left(x_0, x_1, \ldots, x_{l(l-1)-1}, 0, \ldots, 0\right) = circ_{l^2}(1, 0, \ldots, 0),$$

we obtain equations

$$c_0 - c_{l(l-1)} = 1 \text{ and } c_j - c_{l(l-1)+(j \bmod l)} = 0 \text{ for } j = 1, 2, \ldots, l^2 - 1 \tag{6}$$

once again with $c_k = \sum_{\substack{i+j\equiv k \\ (\mathrm{mod}\ l^2)}} a_i x_j$ as in (2).

Write this system down as $\mathbf{T}_\alpha \cdot \left(x_0, x_1, \ldots, x_{l(l-1)-1}\right)^T = (1, 0, \ldots, 0)^T$, where $\mathbf{T}_\alpha$ is square matrix of degree $l(l-1)$ with entries which are linear combinations of a_i. To get proper form of $\mathbf{T}_\alpha$ think of x_j coefficients in equations (6).

For the first column of $\mathbf{T}_\alpha$ we have to observe x_0. In first equation the term x_0 is multiplied by a_0, in equation with c_1 is x_0 multiplied by a_1 and so on, for equation with c_j the term x_0 is multiplied by a_j, thus the first column of $\mathbf{T}_\alpha$ is $\left(a_0, a_1, \ldots, a_{l(l-1)-1}\right)^T$. Note that first row contains coefficients of α.

Observing x_1 we obtain second column. From (2) we see, that the term x_1 could appear in expression of c_0 only with a_8, which does not occur in α. In the term $c_{l(l-1)}$ we have $a_{l(l-1)-1}x_1$. In equation $c_1 + c_{l(l-1)+1} = 0$ we have c_1 with term a_0x_1 and no possible way to get $c_{l(l-1)+1}$ with x_1. Similarly for all equations with c_j where $\gcd(j, l^2) = 1$. In equations where we have c_j and $\gcd(j, l^2) = l$, there we can find $a_{j-1}x_1$ and also $a_{l(l-1)-1}x_1$ in expression of $c_{l(l-1)}$. So the second column is of the form $\left(-a_{l(l-1)-1}, a_0, a_1, \ldots, a_l - a_{l(l-1)-1}, a_{l+1}, \cdots, a_{l(l-1)-2}\right)^T$, which is $\alpha\zeta_{l^2}$ expressed with respect to the power basis of the cyclotomic field $\mathbb{Q}(\zeta_{l^2})$.

In similar way we can show that k-th column of the matrix $\mathbf{T}_\alpha$ consists of coefficients of $\alpha\zeta_{l^2}^{k-1}, k = 1, 2, \ldots, l(l-1)$ expressed with respect to the power basis of the cyclotomic field $\mathbb{Q}(\zeta_{l^2})$.

To every element $\alpha \in \mathbb{Q}(\zeta_{l^2})$ we can assign matrix $\mathbf{T}_\alpha$ or vector $\delta_\alpha = \left(a_0, a_1, \ldots, a_{l(l-1)-1}\right)$. Denote $\mathcal{C}_\mathbf{T}$ set of all such matrices, i.e. $\mathcal{C}_\mathbf{T} = \{\mathbf{T}_\alpha; \alpha \in \mathbb{Q}(\zeta_{l^2})\}$. With this notation we have following theorem

Theorem 1. *For the matrix* $\mathbf{T}_\alpha$ *it holds*

1. $\mathcal{C}_\mathbf{T} \simeq \mathbb{Q}(\zeta_{l^2})$,
2. $\mathbf{T}_\alpha \cdot \delta_\beta = \delta_{\alpha\cdot\beta}$,
3. $\mathrm{N}_{\mathbb{Q}(\zeta_{l^2})/\mathbb{Q}}(\alpha) = |\mathbf{T}_\alpha|$,
4. $\mathrm{Tr}_{\mathbb{Q}(\zeta_{l^2})/\mathbb{Q}} = \mathrm{Tr}(\mathbf{T}_\alpha)$.

Proof. Multiplication by α defines $\mathbb{Q}$-linear transformation

$$t_\alpha : \mathbb{Q}(\zeta_{l^2}) \longrightarrow \mathbb{Q}(\zeta_{l^2}), \quad x \longmapsto \alpha x.$$

The matrix $\mathbf{T}_\alpha$ is its representation with respect to the power integral basis $1, \zeta_{l^2}, \ldots, \zeta_{l^2}^{l(l-1)-1}$. Hence the items $3, 4$ are just definitions of the norm and the trace in $\mathbb{Q}(\zeta_{l^2})$. The rest follows from the discussion above. □

4 Example

In this section we demonstrate the above results on example. Let now $l = 5$, denote $\zeta = \zeta_{l^2}$ and $\alpha = 1 - \zeta^{11} - \zeta^{17}, \beta = 1 + \zeta^{11} - \zeta^{12} \in \mathbb{Q}(\zeta_{l^2})$. Compute the product $\gamma = \alpha\beta$

$$\begin{aligned}
\alpha\beta &= \left(1 - \zeta^{11} - \zeta^{17}\right)\left(1 + \zeta^{11} - \zeta^{12}\right) = 1 + \zeta^{11} - \zeta^{12} - \zeta^{11} - \zeta^{22} + \zeta^{23} - \zeta^{17} - \zeta^{28} + \zeta^{29} \\
&= 1 - \zeta^{12} - \zeta^{22} + \zeta^{23} - \zeta^{17} - \zeta^{3} + \zeta^{4} \\
&= 1 - \zeta^{12} - \left(-\zeta^{2} - \zeta^{7} - \zeta^{12} - \zeta^{17}\right) + \left(-\zeta^{3} - \zeta^{8} - \zeta^{13} - \zeta^{18}\right) - \zeta^{17} - \zeta^{3} + \zeta^{4} \\
&= 1 + \zeta^{2} - 2\zeta^{3} + \zeta^{4} + \zeta^{7} - \zeta^{8} - \zeta^{13} - \zeta^{18}.
\end{aligned} \tag{7}$$

So let now $\mathbf{A}, \mathbf{B} \in \mathcal{C}_{l^2}$ be circulant matrices corresponding to the elements α resp. β and compute their product in $\mathcal{C}_{l^2}$, i.e. that means we have

$$\begin{aligned}
\mathbf{A} &= circ(1,0,0,0,0,0,0,0,0,0,0,0,-1,0,0,0,0,0,-1,0,0,0,0,0,0,0,0), \\
\mathbf{B} &= circ(1,0,0,0,0,0,0,0,0,0,0,0,1,-1,0,0,0,0,0,0,0,0,0,0,0,0,0), \\
\mathbf{C} &= circ(1,0,0,-1,1,0,0,0,0,0,0,0,-1,0,0,0,0,0,-1,0,0,0,0,0,-1,1,0).
\end{aligned}$$

Clearly $\mathbf{C}$ is an element of the ring $\mathcal{C}_{25}$ but not an element of the field $\mathcal{C}_{25}^*$. In this form it represents the product $\alpha\beta$ before we reduced the terms $-\zeta^{28}$ and ζ_{29} in equations (7).

Replacing the term ζ^{22} by $(-\zeta^2-\zeta^7-\zeta^{12}-\zeta^{17})$ in (7) leads to expressing γ with respect to the power basis, in the matrix case this is done just by substracting proper matrix $\mathbf{C}^{\times}$ from the ideal $\mathcal{I}_{25}$, i.e.

$$\begin{aligned}\mathbf{C}^{*} &= \mathbf{C}-\mathbf{C}^{\times}= \\ &= circ(1,0,0,-1,1,0,0,0,0,0,0,0,-1,0,0,0,0,-1,0,0,0,0,-1,1,0)- \\ &\quad - circ(0,0,-1,1,0,0,0,-1,1,0,0,0,-1,1,0,0,0,-1,1,0,0,0,-1,1,0) \\ &= circ(1,0,1,-2,1,0,0,1,-1,0,0,0,0,-1,0,0,0,0,-1,0,0,0,0,0,0).\end{aligned} \tag{8}$$

Notice here that substracting matrix $\mathbf{C}^{\times}$ from matrix $\mathbf{C}$ in (8) is nothing else as computing the product $\mathbf{A}*\mathbf{B}$ as it was defined in (5).

Now we have $\mathbf{C}^{*}\in\mathcal{C}_{25}^{*}$ with the first row entries equal to coefficients of $\gamma=\alpha\beta\in\mathbb{Q}\left(\zeta_{25}\right)$.

The norms of α,β are $\mathrm{N}_{\mathbb{Q}\left(\zeta_{l^2}\right)/\mathbb{Q}}(\alpha)=401$ resp. $\mathrm{N}_{\mathbb{Q}\left(\zeta_{l^2}\right)/\mathbb{Q}}(\beta)=101$, but the determinants are $|\mathbf{A}|=-4411$ resp. $|\mathbf{B}|=1111$. This is because the eigenvalues λ_i with $\gcd(i,l)\neq 1$ belongs to $\mathbb{Q}\left(\zeta_5\right)$ and are not conjugates of λ_j with $\gcd(j,l)=1$ in the field $\mathbb{Q}\left(\zeta_{25}\right)$.

That is the reason for using matrices $\mathbf{T}_{\alpha}$ from $\mathcal{C}_{\mathbf{T}}$. Here, in case of $\alpha=1-\zeta^{11}-\zeta^{17}$, and $\beta=1+\zeta^{11}-\zeta^{12}\in\mathbb{Q}\left(\zeta_{l^2}\right)$, we have

$$\mathbf{T}_{\alpha}\cdot\delta_{\beta}=\begin{pmatrix}
1&0&0&1&0&0&0&0&-1&1&0&0&0&0&-1&0&0&0&0&0\\
0&1&0&0&1&0&0&0&0&-1&1&0&0&0&0&-1&0&0&0&0\\
0&0&1&0&0&1&0&0&0&0&-1&1&0&0&0&0&-1&0&0&0\\
0&0&0&1&0&0&1&0&0&0&0&-1&1&0&0&0&0&-1&0&0\\
0&0&0&0&1&0&0&1&0&0&0&0&-1&1&0&0&0&0&-1&0\\
0&0&0&1&0&1&0&0&0&1&0&0&0&-1&0&0&0&0&0&-1\\
0&0&0&0&1&0&1&0&0&0&1&0&0&0&-1&0&0&0&0&0\\
0&0&0&0&0&1&0&1&0&0&0&1&0&0&0&-1&0&0&0&0\\
0&0&0&0&0&0&1&0&1&0&0&0&1&0&0&0&-1&0&0&0\\
0&0&0&0&0&0&0&1&0&1&0&0&0&1&0&0&0&-1&0&0\\
0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&-1&0\\
-1&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&-1\\
0&-1&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0\\
0&0&-1&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0\\
0&0&0&-1&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&0\\
0&0&0&1&-1&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&1&-1&0&0&0&0&1&0&0&0&0&0&1&0&0&0\\
-1&0&0&0&0&1&-1&0&0&0&0&1&0&0&0&0&0&1&0&0\\
0&-1&0&0&0&0&1&-1&0&0&0&0&1&0&0&0&0&0&1&0\\
0&0&-1&0&0&0&0&1&-1&0&0&0&0&1&0&0&0&0&0&1
\end{pmatrix}\cdot\begin{pmatrix}1\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{pmatrix}=\begin{pmatrix}1\\0\\1\\-2\\1\\0\\0\\0\\1\\-1\\0\\0\\0\\-1\\0\\0\\0\\0\\0\\-1\\0\end{pmatrix}=\delta_{\gamma}.$$

This way we obtain $\gamma=\alpha\beta$ only by using basic matrix operations and not the arithmetics of algebraic number fields. Moreover $|\mathbf{T}_{\alpha}|=401=\mathrm{N}_{\mathbb{Q}\left(\zeta_{25}\right)/\mathbb{Q}}\left(\alpha\right)=401$.

Conclusion

In the presented paper the relation between the ring of circulant matrices, $\mathcal{C}_n$. It is shown that constructing its factor field $\mathcal{C}_{l^2}^{*}=\mathcal{C}_{l^2}/\mathcal{I}_{l^2}$ yields a field isomorphic to the l^2-th cyclotomic field of degree $\varphi(l^2)$ for odd prime l is shown.

All obtained relations are used to representation of elements of cyclotomic field in order to simplify computations in cyclotomic field.

References

[1] V. Dubovský. "A note on circulant matrices of degree 9", *Systemy Wspomagania W Inzynierii Produkcji*, Vol. 6, issue 4, 2017, p. 243–251.

[2] J. Kostra. "A Note on Representation of Cyclotomic Fields", *Acta Mathematica et Informatica Universitatis Ostraviensis*, Vol. 4, 1996, p. 29–35.

[3] M. Pomp, R. Havelek. "On representation of cyclotomic fields $\mathbb{Q}(\zeta_{pq})$", *Acta Mathematica et Informatica Universitatis Ostraviensis*, Vol. 7, 1999, p. 71–78.

O CIRKULANTNÍCH MATICÍCH STUPNĚ l^2

Abstrakt (Streszczenie): Cirkulantní matice mají širokou škálu aplikací v mnoha různých odvětvích matematiky, jako jsou analýza dat a časový řad, zpracování signálů či Fourierova transformace. Další výsledky využívající vlastností cirkulantních matic můžeme nalézt také v algebraické teorii čísel, což je dáno tím, že z okruhu cirkulantních matic prvočíselného stupně p, lze vytvořit faktorový okruh isomorfní s p-tým cyklotomickým tělesem, $\mathbb{Q}(\zeta_p)$. V článku je ukázán vztah mezi okruhem cirkulantních matic stupně l^2, tj. C_{l^2}, kde l je liché prvočíslo, a cyklotomickým tělesem $\mathbb{Q}(\zeta_{l^2})$.

Klíčová slova (Słowa kluczowe): cirkulantní matice, cyklotomické těleso.