2017
Volume 6
issue 4

33

A NOTE ON CIRCULANT MATRICES OF DEGREE 9

33.1 INTRODUCTION

To start with, recall the definition and basic properties of circulant matrices. The 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

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

It is obvious that such matrix is fully determined by its first row, so it is often denoted by $\mathbf{A} = circ_n\left(a_0, a_1, \ldots, a_{n-1}\right)$, and so it will be throughout this paper. From the elements a_i the matrix entry on j-th row and k-th column, i.e. the a_{jk}, could be computed as follows

$$a_{jk} = a_{k-j \pmod n}.$$

We could easily observe that sum and product of two circulant matrices is also circulant matrix and thus the set of all circulant matrices of degree n, denoted by $\mathcal{C}_n$, forms a ring.

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

$$\mathbf{F}_n = \left(\frac{\zeta_n^{ij}}{\sqrt{n}}\right)_{i,j=0,1,\ldots,n-1},$$

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

Now let $\mathbf{D} = \mathbf{FAF}^{-1}$, with $\mathbf{F}$ the Fourier matrix of degree n and the circulant matrix $\mathbf{A} = circ_n(a_0, a_1, \ldots, a_{n-1})$ then $\mathbf{D}$ is a diagonal matrix with entries λ_i being eigenvalues of the matrix $\mathbf{A}$ and equal to

$$\lambda_i = a_0 + a_1\zeta_n^i + a_2\zeta_n^{2i} + \cdots + a_{n-1}\zeta_n^{i(n-1)}. \tag{33.1}$$

Since the Fourier matrix $\mathbf{F}$ is unitary, so the determinants $|\mathbf{A}|$ and $|\mathbf{D}|$ are equal and we could write $|\mathbf{A}| = \prod_{i=0}^{n-1}\lambda_i$. For $i = 0$ we hawe $\lambda_0 = a_0 + a_1 + \cdots + a_{n-1}$ and λ_i for $i = 1, 2, \ldots, n-1$ could be viewed as elements of the n-th cyclotomic field $\mathbb{Q}(\zeta_n)$.

Since this connection is established, we could try to use circulant matrices to represent the elements and the arithmetics of the field $\mathbb{Q}(\zeta_n)$.

This could be done quite straightforward in the case of $n = l$, l is odd prime, because in this case all λ_i for $i = 1, 2, \ldots, l-1$ are conjugates and

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

where $\mathrm{N}_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\alpha)$ denotes the norm of the element $\alpha \in \mathbb{Q}(\zeta_l)$.

The problem left to solve in this case is that, the set $1, \zeta_l, \zeta_l^2, \ldots, \zeta_l^{l-1}$ is not the integral basis of $\mathbb{Q}(\zeta_l)$. From the l-th cyclotomic polynomial $\Phi_l(x) = 1 + x + x^2 + \cdots + x^{l-1}$ we see $\zeta_l + \zeta_l^2 + \cdots + \zeta_l^{l-1} = -1$. Thus we could form the basis $\zeta_l, \zeta_l^2, \ldots, \zeta_l^{l-1}$, which is the normal integral basis of $\mathbb{Q}(\zeta_l)$. The representation of $\mathbb{Q}(\zeta_l)$ is then derived via constructing factor ring of $\mathcal{C}_l$. For further details see paper [1].

In the case of $n = pq$, with two odd primes p, q, we deal with problems such as the elements λ_i with $i \equiv 0 \pmod{p}$ belongs to $\mathbb{Q}(\zeta_q)$, λ_i with $i \equiv 0 \mod q$ belongs to $\mathbb{Q}(\zeta_p)$, and only λ_i with $\gcd(i, n) = 0$ belongs to $\mathbb{Q}(\zeta_n)$. But once again choosing the proper normal integral basis, ζ_n^i with i coprime to n, and using more quite tedious work we obtain representation of the field $\mathbb{Q}(\zeta_n)$ (see [2]).

The purpose of this paper is to show similiar way to represent the field $\mathbb{Q}(\zeta_9)$. Unfortunately for $n = 9$, and further on for $n = l^2$, the n-th cyclotomic field is not tamely ramified. Because of this it does not pose normal integral basis and has to work with power integral basis.

33.2 BASIC OBSERVATIONS

The degree of the field $\mathbb{Q}(\zeta_9)$ is $[\mathbb{Q}(\zeta_9) : \mathbb{Q}] = \varphi(9) = 6$, its basis consists of elements $1, \zeta_9, \zeta_9^2, \ldots, \zeta_9^5$ and every element $\gamma \in \mathbb{Q}(\zeta_9)$ could be written in the form $\gamma = c_0 + c_1\zeta_9 + c_2\zeta_9^2 + \cdots + c_5\zeta_9^5$. Galois group of the extension $\mathbb{Q}(\zeta_9)/\mathbb{Q}$ is generated by the automorphism

$$\phi : \mathbb{Q}(\zeta_9) \longrightarrow \mathbb{Q}(\zeta_9), \quad \phi : \zeta_9 \longmapsto \zeta_9^2,$$

and is isomorphic with the multiplicative group $\left(\mathbb{Z}_9^{\times}, \cdot\right)$.

Now observe how γ conjugate $\phi(\gamma)$ looks like.

$$\phi(\gamma) = c_0 + c_1\zeta_9^2 + c_2\left(\zeta_9^2\right)^2 + \cdots + c_5\left(\zeta_9^2\right)^5 = c_0 + c_1\zeta_9^2 + c_2\zeta_9^4 + c_3\zeta_9^6 + c_4\zeta_9^8 + c_5\zeta_9^{10}.$$

Using the fact $\zeta_9^9 = 1$, it is possible to replace ζ_9^{10} by ζ_9, but to replace $\zeta_9^6, \zeta_9^7, \zeta_9^8$ we have to use cyclotomic polynomial $\Phi_9(x) = 1 + x^3 + x^6$. With the equality $\Phi_9(\zeta_9) = 1 + \zeta_9^3 + \zeta_9^6 = 0$ we could write

$$\zeta_9^6 = -1 - \zeta_9^3, \quad \zeta_9^7 = -\zeta_9 - \zeta_9^4, \quad \zeta_9^8 = -\zeta_9^2 - \zeta_9^5 \tag{33.2}$$

and similarly for higher powers. So we get

$$\phi(\gamma) = (c_0 - c_3) + c_5\zeta_9 + (c_1 - c_4)\zeta_9^2 - c_3\zeta_9^3 + c_2\zeta_9^4 - c_4\zeta_9^5.$$

In the same manner we obtain complete set of γ conjugates, denoted by γ_i for $i = 1, 2, \ldots 6$, with $\gamma_1 = \gamma, \gamma_2 = \phi(\gamma_1)$ and so on.

Let now $\mathbf{A}$ be circulant matrix of degree 9, $\mathbf{A} = circ_9(a_0, a_1, \ldots, a_8)$. As mentioned above the eigenvalues of the matrix $\mathbf{A}$ are elements of the field $\mathbb{Q}(\zeta_9)$. This relationship leads us to the idea of finding homomorphism between the ring $\mathcal{C}_9$ and the field $\mathbb{Q}(\zeta_9)$.

Define mapping ψ as follows

$$\psi : \mathcal{C}_9 \longrightarrow \mathbb{Q}(\zeta_9), \quad \psi : \mathbf{A} \longmapsto a_0 + a_1\zeta_9 + a_2\zeta_9^2 + \cdots + a_8\zeta_9^8.$$

To prove that ψ is a homomorphism, we have to check that $\psi(\mathbf{A} + \mathbf{B}) = \psi(\mathbf{A}) + \psi(\mathbf{B})$ and that $\psi(\mathbf{A} \cdot \mathbf{B}) = \psi(\mathbf{A}) \cdot \psi(\mathbf{B})$. The first part is obvious.

To prove second one, observe that for the matrices $\mathbf{A} = circ_9(a_0, a_1, \ldots, a_8)$, $\mathbf{B} = circ_9(b_0, b_1, \ldots, b_8)$ and $\mathbf{C} = \mathbf{A} \cdot \mathbf{B} = circ_9(c_0, c_1, \ldots, c_8)$ we have

$$c_k = \sum_{\substack{i+j \equiv k \\ (\mathrm{mod}\ 9)}} a_i b_j. \tag{33.3}$$

Multiplying elements $\alpha, \beta \in \mathbb{Q}(\zeta_9)$, with $\alpha = a_0 + a_1\zeta_9 + \cdots + a_8\zeta_9^8$ and $\beta = b_0 + b_1\zeta_9 + \cdots + b_8\zeta_9^8$, we get $\gamma = c_0 + c_1\zeta_9 + \cdots + c_8\zeta_9^8$, with coefficients c_k satisfying the equation (33.3). This is because now we do not expressing elements in power basis and ζ_9 exponents are reduced only by $\zeta_9^9 = 1$, i.e. modulo 9.

Surely the image of ψ is entire field $\mathbb{Q}(\zeta_9)$, so ψ is surjective. The example of the matrices $circ_9(0, 0, \ldots, 0) \neq circ_9(1, 1, \ldots, 1)$ with $\psi(circ_9(0, 0, \ldots, 0)) = 0$ and $\psi(circ_9(1, 1, \ldots, 1)) = 0$ shows, that ψ is not injective.

Natural question arises here - what is the kernel of this homomorphism? Using the equations (33.2) we could show that

$$\begin{aligned} \psi(circ_9(x, y, z, x, y, z, x, y, z)) &= x + y\zeta_9 + z\zeta_9^2 + x\zeta_3\zeta_9^3 + \cdots + y\zeta_9^7 + z\zeta_9^8 = \\ &= x + y\zeta_9 + z\zeta_9^2 + x\zeta_3\zeta_9^3 + \cdots + y\left(-\zeta_9 - \zeta_9^4\right) + z\left(-\zeta_9^2 - \zeta_9^5\right) = 0. \end{aligned} \tag{33.4}$$

From (33.4) we conclude how the kernel, $\ker(\psi)$, of the homomorphism ψ looks like. It is the set $\mathcal{I}_9 = \{circ_9\,(x, y, z, x, y, z, x, y, z)\,; x, y, z \in \mathbb{Q}\}$.

As the set $\mathcal{I}_9$ is ideal in $\mathcal{C}_9$, we could construct a factor ring $\mathcal{C}_9/\mathcal{I}_9$. Every class of this factor ring contains exactly one element of the form $circ_9\,(c_0, c_1, \ldots, c_5, 0, 0, 0)$, which represents $\gamma = c_0 + c_1\zeta_9 + \cdots + c_5\zeta_9^5 \in \mathbb{Q}\,(\zeta_9)$. Asume that $\gamma \neq 0$ and $\gamma^{-1} = d_0 + d_1\zeta_9 + \cdots + d_5\zeta_9^5 \in \mathbb{Q}\,(\zeta_9)$ is its inverse. If we denote $\bar{\mathbf{C}}$ the class $circ_9\,(c_0, c_1, \ldots, c_5, 0, 0, 0)$ and $\bar{\mathbf{D}}$ the class the matrix $circ_9\,(d_0, d_1, \ldots, d_5, 0, 0, 0)$, then these two classes are inverses in the factor ring $\mathcal{C}_9/\mathcal{I}_9$. This shows that $\mathcal{C}_9/\mathcal{I}_9$ is in fact a field, moreover this field is isomorphic with $\mathbb{Q}\,(\zeta_9)$, i.e. we have $\mathcal{C}_9/\mathcal{I}_9 \simeq \mathbb{Q}\,(\zeta_9)$.

Denote the set of all circulant matrices of the form $\mathbf{A} = circ_9\,(a_0, a_1, \ldots, a_5, 0, 0, 0)$ by $\mathcal{C}_9^*$. Clearly $\psi\,(\mathcal{C}_9^*) = \mathbb{Q}\,(\zeta_9)$ and for $\mathbf{A}, \mathbf{B} \in \mathcal{C}_9^*$ also $\psi\,(\mathbf{A} + \mathbf{B}) = \psi\,(\mathbf{A}) + \psi\,(\mathbf{B})$ holds true. But the product $\mathbf{C} = \mathbf{A} \cdot \mathbf{B}$ need not belong to $\mathcal{C}_9^*$.

So in order to get ring structure on the set $\mathcal{C}_9^*$ we have to define multiplication in another way, let $\mathbf{A} = circ_9\,(a_0, a_1, \ldots, a_5, 0, 0, 0)$ and $\mathbf{B} = circ_9\,(b_0, b_1, \ldots, b_5, 0, 0, 0)$ and α, β corresponding elements in $\mathbb{Q}\,(\zeta_9)$ then let product $\mathbf{A} * \mathbf{B}$ be

$$\begin{aligned}
\mathbf{A} * \mathbf{B} &= circ_9\,(a_0, a_1, \ldots, a_5, 0, 0, 0) * circ_9\,(b_0, b_1, \ldots, b_5, 0, 0, 0) = \\
&= circ_9\,(a_0, \ldots, a_5, 0, 0, 0) \cdot circ_9\,(b_0, \ldots, b_5, 0, 0, 0) - circ_9\,(c_6, c_7, c_8, \ldots, c_6, c_7, c_8) = \\
&= circ_9\,(c_0 - c_6, c_1 - c_7, c_2 - c_8, c_3 - c_6, c_4 - c_7, c_5 - c_8, 0, 0, 0) \in \mathcal{C}_9^*,
\end{aligned}$$

with $c_k = \sum_{\substack{i+j\equiv k \\ (\mathrm{mod}\ 9)}} a_i b_j$ as in (33.3).

Now observe that with the help of (33.3) and (33.4) we could show

$$\begin{aligned}
\psi\,(\mathbf{A} * \mathbf{B}) &= \psi\,(\mathbf{A} \cdot \mathbf{B} - circ_9\,(c_6, c_7, c_8, c_6, c_7, c_8, c_6, c_7, c_8)) = \\
&= \psi\,(\mathbf{A} \cdot \mathbf{B}) - \psi\,(circ_9\,(c_6, c_7, c_8, c_6, c_7, c_8, , c_6, c_7, c_8)) = \\
&= \psi\,(\mathbf{A} \cdot \mathbf{B}) - 0 = \psi\,(\mathbf{A}) \cdot \psi\,(\mathbf{B}) = \alpha \cdot \beta \in \mathbb{Q}\,(\zeta_9)\,,
\end{aligned}$$

which means, that mapping ψ reduced to $\mathcal{C}_9^*$ as follows

$$\psi : \mathcal{C}_9^* \longrightarrow \mathbb{Q}\,(\zeta_9)\,, \quad \psi : \mathbf{A} \longmapsto a_0 + a_1\zeta_9 + a_2\zeta_9^2 + \cdots + a_5\zeta_9^5$$

is homomorphism again. Moreover since the kernel is trivial in this case we have also proved that $(\mathcal{C}_9^*, +, *) \simeq \mathbb{Q}\,(\zeta_9)$.

33.3 REPRESENTION OF THE FIELD $\mathbb{Q}\,(\zeta_9)$

The isomorphisms and representations obtained in previous section is easy to derive and handle, but unsufficient in some ways. For instance if the circulant matrix $\mathbf{C} = circ_9\,(c_0, c_1, \ldots, c_5, 0, 0, 0)$ represents element $\gamma \in \mathbb{Q}\,(\zeta_9)$, then $|\mathbf{C}|$ is not equal to the norm of γ, $\mathrm{N}_{\mathbb{Q}(\zeta_9)/\mathbb{Q}}\,(\gamma)$and the trace of the matrix $\mathbf{C}$ is not equal to the trace of the element γ, $\mathrm{Tr}_{\mathbb{Q}(\zeta_9)/\mathbb{Q}}(\gamma)$. Also multiplication in $\mathcal{C}_9^*$ and work with classes in $\mathcal{C}_9/\mathcal{I}_9$ is quite awkward.

So let now $\alpha = a_0 + a_1\zeta_9 + \cdots + a_5\zeta_9^5$ and $\alpha^{-1} = x_0 + x_1\zeta_9 + \cdots + x_5\zeta_9^5$ be its inverse with corresponding matrices from $\mathcal{C}_9^*$ as described above, then we have equality

$$circ_9(a_0, a_1, \ldots, a_5, 0, 0, 0) * circ_9(x_0, x_1, \ldots, x_5, 0, 0, 0) = circ_9(1, 0, \ldots, 0),$$

which leads to system of linear equations

$$\begin{aligned}
c_0 - c_6 &= a_0x_0 - a_5x_1 - a_4x_2 - a_3x_3 + (-a_2 + a_5)x_4 + (-a_1 + a_4)x_5 = 1,\\
c_1 - c_7 &= a_1x_0 + a_0x_1 - a_5x_2 - a_4x_3 - a_3x_4 + (-a_2 + a_5)x_5 = 0,\\
c_2 - c_8 &= a_2x_0 + a_1x_1 + a_0x_2 - a_5x_3 - a_4x_4 - a_3x_5 = 0,\\
c_3 - c_6 &= a_3x_0 + (a_2 - a_5)x_1 + (a_1 - a_4)x_2 + (a_0 - a_3)x_3 - a_2x_4 - a_1x_5 = 0,\\
c_4 - c_7 &= a_4x_0 + a_3x_1 + (a_2 - a_5)x_2 + (a_1 - a_4)x_3 + (a_0 - a_3)x_4 - a_2x_5 = 0,\\
c_5 - c_8 &= a_5x_0 + a_4x_1 + a_3x_2 + (a_2 - a_5)x_3 + (a_1 - a_4)x_4 + (a_0 - a_3)x_5 = 0,
\end{aligned}$$

where $c_k = \sum_{\substack{i+j\equiv k \\ (\mathrm{mod}\ 9)}} a_ix_j$. Write this system down as

$$\begin{pmatrix}
a_0 & -a_5 & -a_4 & -a_3 & -a_2 + a_5 & -a_1 + a_4\\
a_1 & a_0 & -a_5 & -a_4 & -a_3 & -a_2 + a_5\\
a_2 & a_1 & a_0 & -a_5 & -a_4 & -a_3\\
a_3 & a_2 - a_5 & a_1 - a_4 & a_0 - a_3 & -a_2 & -a_1\\
a_4 & a_3 & a_2 - a_5 & a_1 - a_4 & a_0 - a_3 & -a_2\\
a_5 & a_4 & a_3 & a_2 - a_5 & a_1 - a_4 & a_0 - a_3
\end{pmatrix}
\begin{pmatrix} x_0\\ x_1\\ x_2\\ x_3\\ x_4\\ x_5 \end{pmatrix}
=
\begin{pmatrix} 1\\ 0\\ 0\\ 0\\ 0\\ 0 \end{pmatrix}
\tag{33.5}$$

and denote $\mathbf{T}_\alpha$ the matrix occuring in the above equation (33.5).

To every element $\alpha = a_0 + a_1\zeta_9 + \cdots + a_5\zeta_9^5 \in \mathbb{Q}(\zeta_9)$ assign the matrix $\mathbf{T}_\alpha$ and $\delta_\alpha = (a_0, a_1, \ldots, a_5)$. And let $\mathcal{C}_{\mathbf{T}}$ be set of all such matrices, i.e. $\mathcal{C}_{\mathbf{T}} = \{\mathbf{T}_\alpha; \alpha \in \mathbb{Q}(\zeta_9)\}$. With this notation we have

Theorem 33.1. *For the matrix $\mathbf{T}_\alpha$ it holds*

1. $\mathcal{C}_{\mathbf{T}} \simeq \mathbb{Q}(\zeta_9)$,
2. $\mathbf{T}_\alpha \cdot \delta_\beta = \delta_{\alpha\cdot\beta}$,
3. $\mathrm{N}_{\mathbb{Q}(\zeta_9)/\mathbb{Q}}(\alpha) = |\mathbf{T}_\alpha|$,
4. $\mathrm{Tr}_{\mathbb{Q}(\zeta_9)/\mathbb{Q}}(\alpha) = \mathrm{Tr}(\mathbf{T}_\alpha)$.

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

$$t_\alpha : \mathbb{Q}(\zeta_9) \longrightarrow \mathbb{Q}(\zeta_9), \quad x \longmapsto \alpha x.$$

The matrix $\mathbf{T}_\alpha$ is its representation with respect to the power integral basis $1, \zeta_9, \ldots, \zeta_9^5$. Hence the items $3, 4$ are just definitions of the norm and the trace in $\mathbb{Q}(\zeta_9)$. The rest follows from the discussion above. □

33.4 REPRESENTION OF THE SUBFIELDS OF THE FIELD $\mathbb{Q}(\zeta_9)$

In order to get the representation for $\mathbb{Q}(\zeta_9)$ subfields we would use the equations (33.5) again, but with the elements of the given subfield. As mentioned above the Galois group of $\mathbb{Q}(\zeta_9)$ is isomorphic to multiplicative group $\mathbb{Z}_9^\times$. This group has two subgroups, thus there are two subfields of $\mathbb{Q}(\zeta_9)$. The subgroups are $(\{1,4,7\},\cdot)$ and $(\{1,8\},\cdot)$, and the corresponding subfields are $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}\left(\zeta_9+\zeta_9^{-1}\right)$ respectively.

33.4.1 The field $\mathbb{Q}(\zeta_3) \subset \mathbb{Q}(\zeta_9)$

The field $\mathbb{Q}(\zeta_3)$ is clearly subfield of $\mathbb{Q}(\zeta_9)$, since $\zeta_9^3=\zeta_3$. Its basis consists of $1,\zeta_3$ and every $\alpha\in\mathbb{Q}(\zeta_3)$ could be written in the form $\alpha=a_0+a_1\zeta_3=a_0+a_1\zeta_9^3$. Hence with $(a_0,0,0,a_1,0,0)$ and $(x_0,0,0,x_1,0,0)$ the system of linear equations (33.5) turns to be

$$\begin{pmatrix} a_0 & 0 & 0 & -a_1 & 0 & 0 \\ 0 & a_0 & 0 & 0 & -a_1 & 0 \\ 0 & 0 & a_0 & 0 & 0 & -a_1 \\ a_1 & 0 & 0 & a_0-a_1 & 0 & 0 \\ 0 & a_1 & 0 & 0 & a_0-a_1 & 0 \\ 0 & 0 & a_1 & 0 & 0 & a_0-a_1 \end{pmatrix}\begin{pmatrix} x_0 \\ 0 \\ 0 \\ x_1 \\ 0 \\ 0 \end{pmatrix}$$

This system consists only two equations and could be written in the form

$$\begin{pmatrix} a_0 & -a_1 \\ a_1 & a_0-a_1 \end{pmatrix}\begin{pmatrix} x_0 \\ x_1 \end{pmatrix}=\begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{33.6}$$

Denoting $\mathbf{T}_{\alpha,\mathbb{Q}(\zeta_3)}$ the matrix of system (33.6) and $\delta_{\alpha,\mathbb{Q}(\zeta_3)}=(a_0,a_1)$ we get desired representation of the element $\alpha=a_0+a_1\zeta_3\in\mathbb{Q}(\zeta_3)$.

33.4.2 The field $\mathbb{Q}\left(\zeta_9+\zeta_9^{-1}\right) \subset \mathbb{Q}(\zeta_9)$

In the case of the field $\mathbb{Q}\left(\zeta_9+\zeta_9^{-1}\right)$, the maximal real subfield of $\mathbb{Q}(\zeta_9)$, is the situation complicated by the fact that this field provides only power integral basis formed by elements $1,\left(\zeta_9+\zeta_9^{-1}\right),\left(\zeta_9+\zeta_9^{-1}\right)^2$, i.e. for every element $\alpha\in\mathbb{Q}\left(\zeta_9+\zeta_9^{-1}\right)$

$$\alpha=a_0+a_1\left(\zeta_9+\zeta_9^{-1}\right)+a_2\left(\zeta_9+\zeta_9^{-1}\right)^2 \text{ with } a_0,a_1,a_2\in\mathbb{Q}.$$

But in order to place coefficients into equations (33.5) we have to rewrite this in terms of the power integral basis $1,\zeta_9,\zeta_9^2,\ldots,\zeta_9^5$ of the field $\mathbb{Q}(\zeta_9)$, this means to write

$$\begin{aligned} \zeta_9+\zeta_9^{-1} &= \zeta_9+\zeta_9^8=\zeta_9-\zeta_9^2-\zeta_9^5, \\ \left(\zeta_9+\zeta_9^{-1}\right)^2 &= \zeta_9^2+2+\zeta_9^{16}=2+\zeta_9^2+\zeta_9^7=2-\zeta_9+\zeta_9^2-\zeta_9^4, \end{aligned}$$

and hence

$$\alpha=(a_0+2a_2)+(a_1-a_2)\zeta_9-(a_1-a_2)\zeta_9^2-a_2\zeta_9^4-a_1\zeta_9^5. \tag{33.7}$$

With coefficients of α as in (33.7) the system (33.5) become new system of linear equations

$$\begin{pmatrix} a_0+2a_2 & a_1 & a_2 & 0 & -a_2 & -a_1 \\ a_1-a_2 & a_0+2a_2 & a_1 & a_2 & 0 & -a_2 \\ a_2-a_1 & a_1-a_2 & a_0+2a_2 & a_1 & a_2 & 0 \\ 0 & a_2 & a_1 & a_0+2a_2 & a_1-a_2 & a_2-a_1 \\ -a_2 & 0 & a_2 & a_1 & a_0+2a_2 & a_1-a_2 \\ -a_1 & -a_2 & 0 & a_2 & a_1 & a_0+2a_2 \end{pmatrix} \begin{pmatrix} x_0+2x_2 \\ x_1-x_2 \\ -x_1+x_2 \\ 0 \\ -x_2 \\ -x_1 \end{pmatrix} =$$

$$= \begin{pmatrix} a_0+2a_2 & 2a_1-a_2 & 2a_0-a_1+6a_2 \\ a_1-a_2 & a_0-a_1+3a_2 & -a_0+3a_1-4a_2 \\ a_2-a_1 & -a_0+a_1-3a_2 & a_0-3a_1+4a_2 \\ 0 & 0 & 0 \\ -a_2 & -a_1 & -a_0-3a_2 \\ -a_1 & -a_0-3a_2 & a_2-3a_1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$$

The equations in the above system are linearly dependent, its matrix rank is 3, but using Gauss elimination, substracting multiples of row 5 and 6 from rows $1, 2, 3$, we obtain system of the following form and from it the representing matrix $\mathbf{T}_{\mathbb{Q}\left(\zeta_9+\zeta_9^{-1}\right),\alpha}$

$$\begin{pmatrix} a_0 & -a_2 & -a_1 \\ a_1 & a_0+3a_2 & 3a_1-a_2 \\ a_2 & a_1 & a_0+3a_2 \\ 0 & 0 & 0 \\ -a_2 & -a_1 & -a_0-3a_2 \\ -a_1 & -a_0-3a_2 & a_2-3a_1 \end{pmatrix} \to \mathbf{T}_{\alpha,\mathbb{Q}\left(\zeta_9+\zeta_9^{-1}\right)} = \begin{pmatrix} a_0 & -a_2 & -a_1 \\ a_1 & a_0+3a_2 & 3a_1-a_2 \\ a_2 & a_1 & a_0+3a_2 \end{pmatrix}. \quad (33.8)$$

33.4.3 Subfields representation

Let now K be subfield of $\mathbb{Q}(\zeta_9)$, i.e. $\mathbb{Q}(\zeta_3)$ or $\mathbb{Q}\left(\zeta_9+\zeta_9^{-1}\right)$ respectively, $\mathbf{T}_{\alpha,K}$ and $\delta_{\alpha,K}$ are as in (33.6) resp. in (33.8), and finally $\mathcal{C}_{\mathbf{T},K} = \{\mathbf{T}_{\alpha,K}; \alpha \in K\}$ be the set of all such matrices, then

Theorem 33.2. *For the matrix $\mathbf{T}_\alpha$ it holds*

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

Proof. For the proof we use the same ideas as in the proof of Theorem 1. □

33.5 EXAMPLE

Let now $K = \mathbb{Q}\left(\zeta_9 + \zeta_9^{-1}\right)$ and denote its basis elements $\varepsilon_1 = 1, \varepsilon_2 = \zeta_9 + \zeta_9^{-1}$ and $\varepsilon_3 = \varepsilon_2^2 = \left(\zeta_9 + \zeta_9^{-1}\right)^2$, then the corresponding matrices $\mathbf{T}$ and vectors δ are

$$\mathbf{T}_{\varepsilon_1,K} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \delta_{\varepsilon_1,K} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},$$

$$\mathbf{T}_{\varepsilon_2,K} = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 3 \\ 0 & 1 & 0 \end{pmatrix}, \quad \delta_{\varepsilon_2,K} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},$$

$$\mathbf{T}_{\varepsilon_3,K} = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 3 & -1 \\ 1 & 0 & 3 \end{pmatrix}, \quad \delta_{\varepsilon_3,K} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Computing ε_2^3 as $\mathbf{T}_{\varepsilon_2,K} \cdot \delta_{\varepsilon_3,K}$ or $\mathbf{T}_{\varepsilon_3,K} \cdot \delta_{\varepsilon_2,K}$ yields $(-1, 3, 0)$, i.e. $\varepsilon_2^3 = -1 + 3\varepsilon_2$. From this we may conclude that $\varepsilon_2^3 - 3\varepsilon_2 + 1 = 0$ and that $x^3 - 3x + 1$ is minimal polynomial of $\zeta_9 + \zeta_9^{-1}$ and of the field $\mathbb{Q}\left(\zeta_9 + \zeta_9^{-1}\right)$.

For $\alpha = 3 + 2\left(\zeta_9 + \zeta_9^{-1}\right) + \left(\zeta_9 + \zeta_9^{-1}\right)^2 \in K$ we have

$$\mathbf{T}_{\alpha,K} = 3\mathbf{T}_{\varepsilon_1,K} + 2\mathbf{T}_{\varepsilon_2,K} + \mathbf{T}_{\varepsilon_3,K} = \begin{pmatrix} 3 & -1 & 2 \\ 2 & 6 & 5 \\ 1 & 2 & 6 \end{pmatrix}.$$

Also we could compute $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = |\mathbf{T}_{\alpha,K}| = 89$, $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \mathrm{Tr}(\mathbf{T}_{\alpha,K}) = 15$ and α^2 as

$$\mathbf{T}_{\alpha,K} \cdot \delta_{\alpha,K} = \begin{pmatrix} 3 & -1 & -2 \\ 2 & 6 & 5 \\ 1 & 2 & 6 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} = (5, 23, 13),$$

i.e. $\alpha^2 = 5 + 23\left(\zeta_9 + \zeta_9^{-1}\right) + 13\left(\zeta_9 + \zeta_9^{-1}\right)^2$.

All these computation are easy to handle, since we are using only basic matrix operations and not the arithmetics of algebraic number fields.

REFERENCES

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

A NOTE ON CIRCULANT MATRICES OF DEGREE 9

Abstract: *Circulant matrices provide quite a wide range of applications in many different branches of mathematics, such as data and time-series analysis, signal processing or Fourier transformation.*
Huge number of results concerning circulant matrices could be found in algebraic number theory. This is because we could construct factor ring isomorphic to the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$ *from the ring of circulant matrices degree* p*, where* p *is a prime.*
In this paper the connection between ring of circulant matrices of degree 9*,* $\mathcal{C}_9$*, and the cyclotomic field* $\mathbb{Q}(\zeta_9)$ *is shown.*

Keywords: *circulant matrix, cyclotomic field*

A NOTE ON CIRCULANT MATRICES OF DEGREE 9

Abstrakt: *Cirkulantní matice nabízí 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 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 9*,* $\mathcal{C}_9$*, a devátým cyklotomickým tělesem.*

Klíčová slova: *cirkulantní matice, cyklotomické těleso*

Date of submission of the article to the Editor: 04.2017
Date of acceptance of the article by the Editor: 05.2017

RNDr. Viktor DUBOVSKÝ, Ph.D.,
VŠB – Technical University of Ostrava
Department of Mathematics and Descriptive Geometry
17. listopadu 15, 708 33, Ostrava, Czech Republic
tel.: +420 597 324 152, e-mail: viktor.dubovsky@vsb.cz