Acta Mathematica et Informatica Universitatis Ostraviensis

Juraj Kostra

A note on representation of cyclotomic fields

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 4 (1996), No. 1, 29--35

Persistent URL: http://dml.cz/dmlcz/120502

Terms of use:

© University of Ostrava, 1996

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://project.dml.cz

Acta Mathematica et Informatica Universitatis Ostraviensis 4(1996) 29–35

A Note on Representation of Cyclotomic Fields

JURAJ KOSTRA

Abstract. In the paper it is found the representation of cyclotomic field under the corespondence between circulant matrices and cyclotomic fields.

1991 Mathematics Subject Classification: 11R18

Let $C = \mathrm{circ}_n(c_1, c_2, \ldots, c_n)$ be a circulant matrix of degree n. It is known that for the determinant of C the following assertion holds:
Let $\zeta = e^{\frac{2\pi i}{n}}$, $\gamma = (c_1, c_2, \ldots, c_n)$ and let $p_\gamma(z) = c_1 + c_2 z + \ldots + c_n z^{n-1}$. Then

$$\det C = \prod_{j=1}^{n} p_\gamma(\zeta^{j-1}).$$

This formula gives us a correspondence between circulant matrices and elements of m-th cyclotomic field $Q(\zeta_n)$. The matrix $C = \mathrm{circ}_n(c_1, c_2, \ldots, c_n)$ corresponds to the element $\alpha = c_1 + c_2\zeta_n + \ldots + c_n\zeta_n^{n-1}$ from $Q(\zeta_n)$. In the next we shall deal with a prime degree l. The above formula for the discriminant of a matrix $A = \mathrm{circ}_l(a_1, a_2, \ldots, a_l)$ may be expressed as

$$\det A = (a_1 + a_2 + \ldots + a_l) \cdot N_{Q(\zeta_l)/Q}(\alpha).$$

Clearly the correspondence between circulant matrices of a degree l and elements of $Q(\zeta_l)$ is not injective because the set $\{1, \zeta_l, \ldots, \zeta_l^{l-1}\}$ is not a basis for the field $Q(\zeta_l)$ over Q. For example the element

$$\alpha = a_1 + a_2\zeta_l + a_3\zeta_l^2 + \ldots + a_l\zeta_l^{l-1} = (a_2 - a_1)\zeta_l + (a_3 - a_1)\zeta_l^2 + \ldots + (a_l - a_1)\zeta_l^{l-1}$$

corresponds to both different circulant matrices $\mathrm{circ}_l(a_1, a_2, \ldots, a_l)$ and $\mathrm{circ}_l(0, a_2 - a_1, a_3 - a_1, \ldots, a_l - a_1)$.
Now, by C_l we denote the set of all circulant matrices of the prime degree l. The set C_l is a ring under the operations of matrix addition and matrix multiplication. We define the map ϕ from C_l to the field $Q(\zeta_l)$ in the following way

$$\phi[\mathrm{circ}_l(a_1, a_2, \ldots, a_l)] = a_1 + a_2\zeta_l + \ldots + a_l\zeta_l^{l-1}.$$

Clearly ϕ is a surjective homomorphism from C_l to the field $Q(\zeta_l)$. The kernel of the homomorphism ϕ is the ideal I_l of C_l such that

$$I_l = \{\mathrm{circ}_l(a, a, \ldots, a); a \in Q\}.$$

So we have

$$Q(\zeta_l) \simeq C_l/I_l.$$

For any $\beta \in Q(\zeta_l), \beta = b_1\zeta_l + b_2\zeta_l^2 + \ldots + b_{l-1}\zeta_l^{l-1}$ we denote

$$A_\beta = \mathrm{circ}_l(0, b_1, b_2, \ldots, b_{l-1}).$$

By C_l^* we denote the set of all $A_\beta \in C_l, C_l^* = \{A_\beta; \beta \in Q(\zeta_l)\}$. Every class of C_l/I_l contains exactly one element of the form $A_\beta = \mathrm{circ}_l(0, b_1, b_2, \ldots, b_{l-1})$. Clearly $\phi(C_l^*) = Q(\zeta_l)$ and $\phi(A_\beta + A_\gamma) = \phi(A_\beta) + \phi(A_\gamma)$ for $A_\beta, A_\gamma \in C_l^*$. Define multiplication $*$ on C_l^* in the following way :
Let

$$\beta = b_1\zeta_l + b_2\zeta_l^2 + \ldots + b_{l-1}\zeta_l^{l-1}, \gamma = c_1\zeta_l + c_2\zeta_l^2 + \ldots + c_{l-1}\zeta_l^{l-1}$$

and

$$a_k = \sum_{i+j\equiv k \pmod l} b_i c_j.$$

Then

$$A_\beta * A_\gamma = \mathrm{circ}_l(0, b_1, b_2, \ldots, b_{l-1}) * \mathrm{circ}_l(0, c_1, c_2, \ldots, c_{l-1}) =$$

$$= [\mathrm{circ}_l(0, b_1, b_2, \ldots, b_{l-1}) \cdot \mathrm{circ}_l(0, c_1, c_2, \ldots, c_{l-1}) - \mathrm{circ}_l(a_0, a_0, \ldots, a_0)] =$$

$$= \mathrm{circ}_l(0, a_1 - a_0, a_2 - a_0, \ldots, a_{l-1} - a_0).$$

From

$$\phi(A_\beta * A_\gamma) = \phi[A_\beta \cdot A_\gamma - \mathrm{circ}_l(a_0, a_0, \ldots, a_0)] =$$

$$= \phi(A_\beta \cdot A_\gamma) - \phi[\mathrm{circ}_l(a_0, a_0, \ldots, a_0)] =$$

$$= \phi(A_\beta \cdot A_\gamma) = \phi(A_\beta) \cdot \phi(A_\gamma) = \beta \cdot \gamma$$

we have

$$A_\beta * A_\gamma = A_{\beta \cdot \gamma}.$$

By above the following holds:

$$(C_l^*, +, *) \simeq Q(\zeta_l).$$

Now we consider the representation $(C_l^*, +, *)$ of $Q(\zeta_l)$. The representative of 1 in $(C_l^*, +, *)$ is the circulant matrix $\mathrm{circ}_l(0, -1, -1, \ldots, -1)$ and so if we have nonzero element $\alpha \in Q(\zeta_l)$ which is represented by $\mathrm{circ}_l(0, a_1, a_2, \ldots, a_{l-1}) \in (C_l^*, +, *)$ and $\mathrm{circ}_l(0, x_1, x_2, \ldots, x_{l-1}) \in (C_l^*, +, *)$ is the representant of α^{-1} then

$$\mathrm{circ}_l(0, a_1, a_2, \ldots, a_{l-1}) * \mathrm{circ}_l(0, x_1, x_2, \ldots, x_{l-1}) =$$

$$= \mathrm{circ}_l(0, t_1 - t_0, t_2 - t_0, \ldots, t_{l-1} - t_0) = \mathrm{circ}_l(0, -1, -1, \ldots, -1),$$

where

$$t_k = \sum_{i+j\equiv k \pmod l} a_i x_j.$$

We have got a system of linear equations τ

$$t_k - t_0 = -1$$

for all $k = 1, 2, \ldots, l-1$. By this system of equations it follows

$$\begin{pmatrix} -a_{l-1} & a_{l-1} - a_{l-2} & a_{l-2} - a_{l-3} & \cdots & a_2 - a_1 \\ a_1 - a_{l-1} & -a_{l-2} & a_{l-1} - a_{l-3} & \cdots & a_3 - a_1 \\ \vdots & \vdots & \ddots & \vdots & \\ a_{l-2} - a_{l-1} & a_{l-3} - a_{l-2} & a_{l-4} - a_{l-3} & \cdots & -a_1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{l-1} \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \\ \vdots \\ -1 \end{pmatrix}$$

We denote

$$T_\alpha = \begin{pmatrix} -a_{l-1} & a_{l-1} - a_{l-2} & a_{l-2} - a_{l-3} & \cdots & a_2 - a_1 \\ a_1 - a_{l-1} & -a_{l-2} & a_{l-1} - a_{l-3} & \cdots & a_3 - a_1 \\ \vdots & \vdots & \ddots & \vdots & \\ a_{l-2} - a_{l-1} & a_{l-3} - a_{l-2} & a_{l-4} - a_{l-3} & \cdots & -a_1 \end{pmatrix}$$

and

$$\lambda_\alpha = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{l-1} \end{pmatrix},$$

where $a_1, a_2, \ldots, a_{l-1}$ are coordinates of the element α in the basis $\zeta_l, \zeta_l^2, \ldots, \zeta_l^{l-1}$. We denote by

$$C_T = \{T_\alpha; \alpha \in Q(\zeta l)\}.$$

Theorem 1. *For the matrix T_α it holds:*

(1) $C_T \simeq Q(\zeta_l)$

(2) $T_\alpha \cdot \lambda_\beta = \lambda_{\alpha \cdot \beta}$

(3) $\mathrm{Tr}_{Q(\zeta_l)/Q}(\alpha) = \lambda_{-1}^T \cdot T_\alpha \cdot \lambda_{-1}$.

(4) $N_{Q(\zeta_l)/Q}(\alpha) = \det T_\alpha$.

Proof: The matrix T_α is just the matrix corresponding to multiplication by α in the basis Z. □

Now let $Q \subset K \subset Q(\zeta_l), [Q(\zeta_l) : K] = \frac{l-1}{s} = r$,and let $\alpha \in K$ be represented by $\mathrm{circ}_l(0, a_1, a_2, \ldots, a_{l-1}) \in C_l^*$,and $\mathrm{circ}_l(0, x_1, x_2, \ldots, x_{l-1}) \in C_l^*$ be the representative of α^{-1}. By definition of K, the element $\varepsilon = \mathrm{Tr}_{Q(\zeta_l)/K}(\zeta_l)$ generates an integral normal basis for K/Q. Let $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_s$ be this integral normal basis

$$\varepsilon_1 = \sum_{i \in M_1} \zeta_l^i, \varepsilon_2 = \sum_{i \in M_2} \zeta_l^i, \ldots, \varepsilon_s = \sum_{i \in M_s} \zeta_l^i,$$

where $M_j \in G(Q(\zeta_l)/Q)/G(Q(\zeta_l)/K)$ and so for circulant matrices $\mathrm{circ}_l(0, a_1, a_2, \ldots, a_{l-1})$, $\mathrm{circ}_l(0, x_1, x_2, \ldots, x_{l-1})$ we have

$$a_i = a_k\,,\, x_i = x_k$$

for $i, k \in M_j, j \in \{1, 2, \ldots, l-1\}$.
Now if we take the first s different equations of system τ (coresponding to the system of representatives of sets $M_i, i = 1, 2, \ldots, s$), we get a new system τ_K. Any equation of τ_K contains s different elements x_i which will be denoted $y_1, y_2, \ldots, y_s$. The matrix of this system we denote $T_{\alpha,K}$.We get

$$T_{\alpha,K} \cdot \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_s \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \\ \vdots \\ -1 \end{pmatrix}$$

Denote

$$\lambda_{\alpha,K} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_s \end{pmatrix},$$

where $a_1, a_2, \ldots, a_s$ are coordinates of the element α in the basis $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_s$. Denote

$$C_{T,K} = \{T_{\alpha,K}; \alpha \in K\}.$$

Theorem 2. *For the matrix $T_{\alpha,K}$ it holds:*

(1) $C_{T,K} \simeq K$

(2) $T_{\alpha,K} \cdot \lambda_{\beta,K} = \lambda_{\alpha\cdot\beta,K}$

(3) $\mathrm{Tr}_{K/Q}(\alpha) = \lambda^T_{-1,K} \cdot T_{\alpha,K} \cdot \lambda_{-1,K}$.

(4) $N_{K/Q}(\alpha) = \det T_{\alpha,K}$.

PROOF: The proof is by the same way as the proof of Theorem 1. □

Remark. If we generate $T_{\varepsilon_1,K}, T_{\varepsilon_2,K}, \ldots, T_{\varepsilon_s,K}$, then for $\alpha = a_1 \cdot \varepsilon_1 + a_2 \cdot \varepsilon_2 + \cdots + a_s \cdot \varepsilon_s$ we have $T_{\alpha,K} = a_1 \cdot T_{\varepsilon_1,K} + a_2 \cdot T_{\varepsilon_2,K} + \ldots + a_s \cdot T_{\varepsilon_s,K}$.

Example. Let $l = 7, Q \subset K \subset Q(\zeta_l), [K : Q] = 3$ then

$$\varepsilon_1 = \zeta_7 + \zeta_7^6, \varepsilon_2 = \zeta_7^2 + \zeta_7^5, \varepsilon_3 = \zeta_7^3 + \zeta_7^4$$

We have

$$T_{\varepsilon_1} = \begin{pmatrix} -1 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & -1 \\ -1 & 1 & 0 & 1 & 0 & -1 \\ -1 & 0 & 1 & 0 & 1 & -1 \\ -1 & 0 & 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}$$

$$T_{\varepsilon_2} = \begin{pmatrix} 0 & -1 & 1 & 0 & -1 & 1 \\ 0 & -1 & 0 & 1 & -1 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 \\ 0 & -1 & 1 & 0 & -1 & 0 \\ 1 & -1 & 0 & 1 & -1 & 0 \end{pmatrix}$$

$$T_{\varepsilon_3} = \begin{pmatrix} 0 & 0 & -1 & 0 & 1 & 0 \\ 0 & 0 & -1 & -1 & 1 & 1 \\ 0 & 0 & -1 & -1 & 0 & 1 \\ 1 & 0 & -1 & -1 & 0 & 0 \\ 1 & 1 & -1 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 \end{pmatrix}$$

and so

$$T_{\varepsilon_1,K} = \begin{pmatrix} -2 & 1 & 0 \\ -1 & 0 & 1 \\ -2 & 1 & 1 \end{pmatrix}$$

$$T_{\varepsilon_2,K} = \begin{pmatrix} 1 & -2 & 1 \\ 0 & -2 & 1 \\ 1 & -1 & 0 \end{pmatrix}$$

$$T_{\varepsilon_3,K} = \begin{pmatrix} 0 & 1 & -1 \\ 1 & 1 & -2 \\ 1 & 0 & -2 \end{pmatrix}.$$

In such a way we get for $\alpha = a_1 \cdot \varepsilon_1 + a_2 \cdot \varepsilon_2 + a_3 \cdot \varepsilon_3$ that

$$T_{\alpha,K} = \begin{pmatrix} a_2 - 2a_1 & a_1 - 2a_2 + a_3 & a_2 - a_3 \\ a_3 - a_1 & a_3 - 2a_2 & a_1 + a_2 - 2a_3 \\ -2a_1 + a_2 + a_3 & a_1 - a_2 & a_1 - 2a_3 \end{pmatrix}$$

For example let $\alpha = 2\varepsilon_1 + 3\varepsilon_2 - \varepsilon_3$, then

$$N_{K/Q}(\alpha) = \begin{vmatrix} -1 & -5 & 4 \\ -3 & -7 & 7 \\ -2 & -1 & 4 \end{vmatrix} = -13.$$

Example. Let $l = 13, Q \subset K \subset Q(\zeta_{13}), [K:Q] = 3$, then

$$\varepsilon_1 = \zeta_{13} + \zeta_{13}^8 + \zeta_{13}^{12} + \zeta_{13}^5, \varepsilon_2 = \zeta_{13}^2 + \zeta_{13}^3 + \zeta_{13}^{11} + \zeta_{13}^{10}, \varepsilon_3 = \zeta_{13}^4 + \zeta_{13}^6 + \zeta_{13}^9 + \zeta_{13}^7$$

For $\alpha = b_1 \cdot \varepsilon_1 + b_2 \cdot \varepsilon_2 + b_3 \cdot \varepsilon_3$

$$T_\alpha = \begin{pmatrix} -a_{12} & a_{12} - a_{11} & a_{11} - a_{10} & \dots & a_2 - a_1 \\ a_1 - a_{12} & -a_{11} & a_{12} - a_{10} & \dots & a_3 - a_1 \\ \vdots & \vdots & \ddots & \vdots & \\ a_{11} - a_{12} & a_{1o} - a_{11} & a_9 - a_{10} & \dots & -a_1 \end{pmatrix}$$

where

$$a_1 = a_5 = a_8 = a_{12} = b_1$$

$$a_2 = a_3 = a_{10} = a_{11} = b_2$$

$$a_4 = a_6 = a_7 = a_9 = b_3$$

and so we have

$$T_\alpha =$$

$$\begin{pmatrix}
-b_1 & b_1-b_2 & 0 & b_2-b_3 & b_3-b_1 & b_1-b_3 & 0 & b_3-b_1 & b_1-b_3 & b_3-b_2 & 0 & b_2-b_1 \\
0 & -b_2 & b_1-b_2 & b_2-b_3 & b_2-b_1 & 0 & b_1-b_3 & b_3-b_1 & 0 & b_1-b_2 & b_3-b_2 & b_2-b_1 \\
b_2-b_1 & b_1-b_2 & -b_2 & b_1-b_3 & b_2-b_1 & b_2-b_3 & 0 & 0 & 0 & b_3-b_2 & b_1-b_2 & b_3-b_1 \\
b_2-b_1 & 0 & b_1-b_2 & -b_3 & 0 & b_2-b_3 & b_2-b_3 & b_3-b_1 & b_1-b_3 & b_3-b_2 & b_3-b_2 & 0 \\
b_3-b_1 & 0 & 0 & b_1-b_3 & -b_1 & b_1-b_3 & b_2-b_3 & b_2-b_1 & 0 & b_1-b_2 & b_3-b_2 & b_3-b_1 \\
0 & b_3-b_2 & 0 & b_2-b_3 & 0 & -b_3 & b_1-b_3 & b_2-b_1 & b_2-b_3 & b_3-b_2 & b_1-b_2 & b_3-b_1 \\
b_3-b_1 & b_1-b_2 & b_3-b_2 & b_2-b_3 & b_2-b_1 & b_1-b_3 & -b_3 & 0 & b_2-b_3 & 0 & b_3-b_2 & 0 \\
b_3-b_1 & b_3-b_2 & b_1-b_2 & 0 & b_2-b_1 & b_2-b_3 & b_1-b_3 & -b_1 & b_1-b_3 & 0 & 0 & b_2-b_1 \\
0 & b_3-b_2 & b_3-b_2 & b_1-b_3 & b_3-b_1 & b_2-b_3 & b_2-b_3 & 0 & -b_3 & b_1-b_2 & 0 & b_2-b_1 \\
b_3-b_1 & b_1-b_2 & b_3-b_2 & 0 & 0 & 0 & b_2-b_3 & b_2-b_1 & b_1-b_3 & -b_2 & b_1-b_2 & b_2-b_1 \\
b_2-b_1 & b_3-b_2 & b_1-b_2 & 0 & b_3-b_1 & b_1-b_3 & 0 & b_2-b_1 & b_2-b_3 & b_1-b_2 & -b_2 & 0 \\
b_2-b_1 & 0 & b_3-b_2 & b_1-b_3 & b_3-b_1 & 0 & b_1-b_3 & b_3-b_1 & b_2-b_3 & 0 & b_1-b_2 & -b_1
\end{pmatrix}$$

For $x \in K$

$$\lambda_x = \begin{pmatrix} x_1 \\ x_2 \\ x_2 \\ x_3 \\ x_1 \\ x_3 \\ x_3 \\ x_1 \\ x_3 \\ x_2 \\ x_2 \\ x_1 \end{pmatrix}$$

If we take the first three different rows of the vector

$$T_\alpha \cdot \lambda_x$$

we get

$$T_{\alpha,K} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} -4b_1 + b_2 + b_3 & b_1 - 2b_2 + b_3 & 2b_1 + b_2 - 3b_3 \\ -3b_1 + 2b_2 + b_3 & 2b_1 - 4b_2 + b_3 & b_1 + b_2 - 2b_3 \\ -2b_1 + b_2 + b_3 & b_1 - 3b_2 + 2b_3 & b_1 + 2b_2 - 4b_3 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

So we have

$$N_{K/Q}(\alpha) = \begin{vmatrix} -4b_1 + b_2 + b_3 & b_1 - 2b_2 + b_3 & 2b_1 + b_2 - 3b_3 \\ -3b_1 + 2b_2 + b_3 & 2b_1 - 4b_2 + b_3 & b_1 + b_2 - 2b_3 \\ -2b_1 + b_2 + b_3 & b_1 - 3b_2 + 2b_3 & b_1 + 2b_2 - 4b_3 \end{vmatrix}$$

Let $\beta = c_1\varepsilon_1 + c_2\varepsilon_2 + c_3\varepsilon_3$. Then coordinates of $\alpha \cdot \beta$ in the basis $\varepsilon_1, \varepsilon_2, \varepsilon_3$ are

$$T_{\alpha,K} \cdot \lambda_{\beta,K} = \begin{pmatrix} -4b_1 + b_2 + b_3 & b_1 - 2b_2 + b_3 & 2b_1 + b_2 - 3b_3 \\ -3b_1 + 2b_2 + b_3 & 2b_1 - 4b_2 + b_3 & b_1 + b_2 - 2b_3 \\ -2b_1 + b_2 + b_3 & b_1 - 3b_2 + 2b_3 & b_1 + 2b_2 - 4b_3 \end{pmatrix} \cdot \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} =$$

$$= \begin{pmatrix} (-4b_1 + b_2 + b_3)c_1 + (b_1 - 2b_2 + b_3)c_2 + (2b_1 + b_2 - 3b_3)c_3 \\ (-3b_1 + 2b_2 + b_3)c_1 + (2b_1 - 4b_2 + b_3)c_2 + (b_1 + b_2 - 2b_3)c_3 \\ (-2b_1 + b_2 + b_3)c_1 + (b_1 - 3b_2 + 2b_3)c_2 + (b_1 + 2b_2 - 4b_3)c_3 \end{pmatrix} = \lambda_{\alpha\cdot\beta}$$

References

[1] Borevich, Z. I., Shafarevich, I. R., *Number Theory*, Moscow (Russian, 3rd ed.) [New York (english translation)], 1964 [1966].

[2] Davis, P. J., *Circulant matrices*, Wiley–Interscience publishers, John Wiley and sons, New York–Chichester–Brisbane–Toronto, 1979.

[3] Newman, M., Taussky, O., *On a generalization of the normal basis in abelian algebraic number fields*, Comm. Pure Appl. Math. **9** (1958), 85–91.

Address: Department of Mathematics, University of Ostrava, Bráfova 7, CZ—701 03 Ostrava, Czech Republic

Paper was supported by grant 09/3418.