Acta Mathematica et Informatica Universitatis Ostraviensis

Marek Pomp; Radim Havelek

On representation of cyclotomic fields $\mathbb{Q}(\zeta_{pq})$

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 7 (1999), No. 1, 71--78

Persistent URL: http://dml.cz/dmlcz/120549

On representation of cyclotomic fields $\mathbb{Q}(\zeta_{pq})$

Marek Pomp
Radim Havelek

Abstract: In this paper is shown representation of cyclotomic fields $\mathbb{Q}(\zeta_{pq})$, where p, q are primes, as the correspondence between circulant matrices and elements of this cyclotomic field.
Key Words: cyclotomic field, circulant matrix, integral normal basis

In the paper [4] it is found a representation of cyclotomic fields $\mathbb{Q}(\zeta_p)$, where, $\zeta_p = \mathrm{e}^{2\pi \mathrm{i}/p}$, p is the prime, as the correspondence between circulant matrices and elements of this cyclotomic field. In the present paper it will be found representation of cyclotomic fields $\mathbb{Q}(\zeta_m)$, where m is product of two distinct primes $m = p \cdot q$.

Correspondence between the set C_n of rational circulant matrices of degree n, $n \in \mathbb{N}$, and n-th cyclotomic field $\mathbb{Q}(\zeta_n)$ is given by map ϕ:

$$\phi\big(\mathrm{circ}(a_0, a_1, \ldots, a_{n-1})\big) = a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta_n^{n-1} \tag{1}$$

Because of the set $\{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}$ is not a basis for the field $\mathbb{Q}(\zeta_n)$ under $\mathbb{Q}$, this map is surjective homomorphism from ring C_n to the field $\mathbb{Q}(\zeta_n)$.

Let $m = p \cdot q$, where p, q are different primes. We denote by C_m the set of circulant matrices of degree m, and $\zeta_m = \mathrm{e}^{2\pi \mathrm{i}/m}$. The set of all primitive roots of unity

$$N_m = \left\{\zeta_m^i;\ i \not\equiv 0 \pmod{p} \text{ and } i \not\equiv 0 \pmod{q}\right\}$$

is an integral normal basis of the field $\mathbb{Q}(\zeta_m)$ under $\mathbb{Q}$ and it holds

$$N_m = \left\{\zeta_m^r;\ \text{where } r \equiv k + l \pmod{m}, k \equiv 0 \pmod{p}, l \equiv 0 \pmod{q}\right\}.$$

Since

$$\zeta_m^{ip} = -1 \sum_{k=1}^{p-1} \zeta_m^{(ip+kq) \pmod{m}}, \qquad i = 1, 2, \ldots, q-1,$$

$$\zeta_m^{jq} = -1 \sum_{l=1}^{q-1} \zeta_m^{(jq+lp) \pmod{m}}, \qquad j = 1, 2, \ldots, p-1,$$

we have, that any element $\alpha \in \mathbb{Q}(\zeta_m)$

$$\alpha = a_0 + a_1\zeta_m + a_2\zeta_m^2 + \cdots + a_{m-1}\zeta_m^{m-1} = \\ = (a_1 - a_0)\zeta_m + (a_2 - a_0)\zeta_m^2 + \cdots + (a_{m-1} - a_0)\zeta_m^{m-1},$$

have unique expression in the form

$$\alpha = \sum_{\substack{r \equiv k+l \pmod m \\ k \equiv 0 \pmod p \\ l \equiv 0 \pmod q}} (a_r + a_0 - a_k - a_l)\zeta_m^r. \tag{2}$$

Proposition 1. *Mapping $\phi : C_m \to \mathbb{Q}(\zeta_m)$, given by (1), have the kernel*

$$I_m = \{\operatorname{circ}(a_0, a_1, \ldots, a_{m-1});\ \text{where } a_r = a_k + a_l - a_0, \\ \text{for } r \equiv k + l \pmod m, k \equiv 0 \pmod p, l \equiv 0 \pmod q\}.$$

Proof. Let $\mathbf{A} \in I_m$, then

$$\phi(\mathbf{A}) = a_0 + \sum_{\substack{r \equiv k+l \pmod m \\ k \equiv 0 \pmod p \\ l \equiv 0 \pmod q}} (a_k + a_l - a_0)\zeta_m^r + \\ + \sum_{k \equiv 0 \pmod p} a_k\zeta_m^k + \sum_{l \equiv 0 \pmod q} a_l\zeta_m^l = \\ = a_0 - a_0 \sum_{\zeta_m^i \in N_m} \zeta_m^i + \\ + \sum_{k \equiv 0 \pmod p} a_k \sum_{l \equiv 0 \pmod q} \zeta_m^{k+l \pmod m} + \\ + \sum_{l \equiv 0 \pmod q} a_l \sum_{k \equiv 0 \pmod p} \zeta_m^{l+k \pmod m}.$$

Since

$$\sum_{\zeta_m^i \in N_m} \zeta_m^i = 1,$$

$$\sum_{l \equiv 0 \pmod q} \zeta_m^{k+l \pmod m} = \zeta_m^k \sum_{l \equiv 0 \pmod q} \zeta_m^l = 0, \qquad \text{where } k \equiv 0 \pmod p,$$

$$\sum_{k \equiv 0 \pmod p} \zeta_m^{l+k \pmod m} = \zeta_m^l \sum_{k \equiv 0 \pmod p} \zeta_m^k = 0, \qquad \text{where } l \equiv 0 \pmod q,$$

it holds $\phi(\mathbf{A}) = 0$ and so $I_m \subseteq \ker \phi$. Reverse inclusion yields obviously from (2). □

Let C_m^* be a subset of the set C_m,

$$C_m^* = \{\operatorname{circ}(a_0, a_1, \ldots, a_{m-1}); \\ \text{where } a_i = 0 \text{ for every } i \equiv 0 \pmod p \text{ or } i \equiv 0 \pmod q\}.$$

Any class of the factor-field C_m/I_m contains one and only one element of C_m^*. If matrices $\mathbf{A}, \mathbf{B}$ are the elements of the set C_m^*, and

$$\mathbf{A} \cdot \mathbf{B} = \operatorname{circ}(c_0, c_1, \ldots, c_{m-1}),$$

we denote by $\mathbf{C_{AB}}$ the matrix from ideal I_m, $\mathbf{C_{AB}} = \operatorname{circ}(d_0, d_1, \ldots, d_{m-1})$, where $d_i = c_i$ for every $i \equiv 0 \pmod p$ or $i \equiv 0 \pmod q$. Next we define the relation $*$ on the set C_m^*

$$\mathbf{A} * \mathbf{B} \stackrel{\text{def}}{=} \mathbf{A} \cdot \mathbf{B} - \mathbf{C_{AB}}.$$

For the map ϕ it holds:

$$\phi(\mathbf{A} * \mathbf{B}) = \phi(\mathbf{A} \cdot \mathbf{B}) - \phi(\mathbf{C_{AB}}) = \phi(\mathbf{A} \cdot \mathbf{B}).$$

Proposition 2. *The set C_m^* under obvious matrix operation $+$ and operation $*$ is the field and*

$$(C_m^*, +, *) \simeq (C_m/I_m, +, \cdot) \simeq \mathbb{Q}(\zeta_m).$$

Now we look on the multiplication in $\mathbb{Q}(\zeta_m)$, $m = p \cdot q$, where p, q are distinct primes.

Let the representative of $\alpha \in \mathbb{Q}(\zeta_m)$ be the matrix $\mathbf{A} = \operatorname{circ}(a_0, a_1, \ldots, a_{m-1})$ and the representative of $\beta \in \mathbb{Q}(\zeta_m)$ be the matrix $\mathbf{B} = \operatorname{circ}(b_0, b_1, \ldots, b_{m-1})$, $\mathbf{A}, \mathbf{B} \in \in C_m^*$. We denote by λ'_β vector of elements of matrix $\mathbf{B}$, $\lambda'_\beta = (b_0, b_1, \ldots, b_{m-1})^{\mathrm{T}}$. Let $\lambda'_{\alpha\cdot\beta} = (d_0, d_1, \ldots, d_{m-1})^{\mathrm{T}}$ is the vector of elements of the matrix $\mathbf{A} * \mathbf{B}$, i.e. representative of product $\alpha \cdot \beta$. Then there is the matrix $\mathbf{T}'_\alpha(t_{rs})$ so that

$$\mathbf{T}'_\alpha \cdot \lambda'_\beta = \lambda'_{\alpha\cdot\beta}.$$

The elements of matrix $\mathbf{A} * \mathbf{B}$ we can express to

$$d_r = \begin{cases} 0 & \text{if } r \equiv 0 \pmod p \text{ or } r \equiv 0 \pmod q, \\ c_r + c_0 - c_k - c_l & \text{in the other cases,} \end{cases}$$

where c_i are elements of product $\mathbf{A} \cdot \mathbf{B} = \operatorname{circ}(c_0, c_1, \ldots c_{m-1})$,

$$c_i = \sum_{j_1 + j_2 \equiv i \pmod m} a_{j_1} b_{j_2},$$

and $r \equiv k + l \pmod m$, $k \equiv 0 \pmod p$, $l \equiv 0 \pmod q$. If

$$\begin{aligned} d_r &= \sum_{s=1}^{m-1} t_{rs} b_s = \\ &= \sum_{i+j \equiv r \pmod m} a_i b_j + \sum_{i+j \equiv 0 \pmod m} a_i b_j - \\ &\quad - \sum_{i+j \equiv k \pmod m} a_i b_j - \sum_{i+j \equiv l \pmod m} a_i b_j. \end{aligned} \tag{3}$$

then we express the elements of matrix $\mathbf{T}'_\alpha$

$$t_{rs} = a_{i_1} + a_{i_2} - a_{i_3} - a_{i_4} \tag{4}$$

where $i_1 \equiv r - s \pmod m$, $i_2 \equiv m - s \pmod m$, $i_3 \equiv k - s \pmod m$ and $i_4 \equiv l - s \pmod m$.

Because of $b_s = 0$ for $s \equiv 0 \pmod p$ or $s \equiv 0 \pmod q$ we can omit s-th columns of matrix $\mathbf{T}'_\alpha$, also $d_r = 0$ for $r \equiv 0 \pmod p$ or $r \equiv 0 \pmod q$ than we can omit r-th rows of matrix $\mathbf{T}'_\alpha$. The new matrix we denote by $\mathbf{T}_\alpha$ and we denote by $C_\mathbf{T}$ the set of all matrix $\mathbf{T}_\alpha$, $\alpha \in \mathbb{Q}(\zeta_m)$. Let λ_β is the vector of nonzero elements of the vector λ'_β. The vector λ_β is vector of coordinates of element β in integral normal basis N_m.

Because of $\mathbf{T}_\alpha$ is matrix of multiplication in regard to the integral normal basis N_m and by Proposition 2 the following theorem holds. (See [1].)

Theorem 1. *Let $\alpha, \beta \in \mathbb{Q}(\zeta_m)$ and let $T_\alpha \in C_\mathbf{T}$ then*

(1) $C_\mathbf{T} \simeq \mathbb{Q}(\zeta_m)$
(2) $\mathbf{T}_\alpha \cdot \lambda_\beta = \lambda_{\alpha\cdot\beta}$
(3) $\mathrm{Tr}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\alpha) = \mathrm{Tr}(\mathbf{T}_\alpha)$
(4) $\mathrm{N}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\alpha) = \det \mathbf{T}_\alpha$

Now, let the field K be the subfield of $\mathbb{Q}(\zeta_m)$ and $[\mathbb{Q}(\zeta_m) : K] = (p-1)(q-1)/w$. An integral normal basis in field K, $N_K = \{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_w\}$, is generate by element $\varepsilon_1 = \mathrm{Tr}_{\mathbb{Q}(\zeta_m)/K}(\zeta_m)$ and

$$\varepsilon_j = \sum_{\sigma \in M_j} \zeta_m^\sigma, \qquad j = 1, 2, \ldots, w$$

where $M_j \in G\big(\mathbb{Q}(\zeta_m)/\mathbb{Q}\big)/G\big(\mathbb{Q}(\zeta_m)/K\big)$. We denote the index set

$$\mathcal{I}_j = \big\{i;\ \zeta_m^i \in \{\zeta_m^\sigma;\ \sigma \in M_j\}\big\}; \qquad j = 1, 2, \ldots w$$

Classes of group $G\big(\mathbb{Q}(\zeta_m)/\mathbb{Q}\big)/G\big(\mathbb{Q}(\zeta_m)/K\big)$ are index in order $M_1, M_2, \ldots, M_w$, where $j_1 < j_2$ if and only if $\min \mathcal{I}_{j_1} < \min \mathcal{I}_{j_2}$.

Let $\alpha, \beta \in K$. The representative of β in $\mathbb{Q}(\zeta_m)$, $\mathrm{circ}(b_0, b_1, \ldots, b_{m-1})$, have $b_{i_1} = b_{i_2}$, where $i_1, i_2 \in \mathcal{I}_j$, $j = 1, 2, \ldots w$.

If $h_i = \min \mathcal{I}_i$, $i = 1, 2, \ldots w$, then equation (3) we can obtain in form

$$d_r = \sum_{i=1}^{w} t'_{ri} b_{h_i},$$

where

$$t'_{ri} = \sum_{j \in \mathcal{I}_i} t_{rj}.$$

Since $r_1, r_2 \in \mathcal{I}_j$, $j = 1, 2, \ldots w$ imply $t'_{r_1 i} = t'_{r_2 i}$, we put $s_{ji} = t'_{ri}$, where $r \in \mathcal{I}_j$. Let $\mathbf{T}_{\alpha,K}$ be a matrix of elements s_{ji}, $j, i = 1, 2, \ldots w$. We denote by $C_{\mathbf{T},K}$ the set of all matrix $\mathbf{T}_{\alpha,K}$, $\alpha \in K$. Let $\lambda_{\alpha,K}$ is the vector of coordinates of an element $\alpha \in K$, in the basis $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_w$.

The following theorem holds by the same way as Theorem 1.

Theorem 2. *Let $\alpha, \beta \in K \subseteq \mathbb{Q}(\zeta_m)$ and let $T_{\alpha,K} \in C_{\mathbf{T},K}$ then*

(1) $C_{\mathbf{T},K} \simeq K$
(2) $\mathbf{T}_{\alpha,K} \cdot \lambda_{\beta,K} = \lambda_{\alpha\cdot\beta,K}$
(3) $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \mathrm{Tr}(\mathbf{T}_{\alpha,K})$
(4) $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \det \mathbf{T}_{\alpha,K}$

Example. Let $p = 3$, $q = 5$. Let $\alpha \in \mathbb{Q}(\zeta_{15})$,

$$\alpha = a_1\zeta_{15} + a_2\zeta_{15}^2 + a_4\zeta_{15}^4 + a_7\zeta_{15}^7 + a_8\zeta_{15}^8 + a_{11}\zeta_{15}^{11} + a_{13}\zeta_{15}^{13} + a_{14}\zeta_{15}^{14}.$$

From (4) we obtain the matrix $\mathbf{T}_\alpha$. It is presented at page 76.

For every $\beta \in \mathbb{Q}(\zeta_{15})$

$$\beta = b_1\zeta_{15} + b_2\zeta_{15}^2 + b_4\zeta_{15}^4 + b_7\zeta_{15}^7 + b_8\zeta_{15}^8 + b_{11}\zeta_{15}^{11} + b_{13}\zeta_{15}^{13} + b_{14}\zeta_{15}^{14}.$$

holds

$$\mathbf{T}_\beta = b_1\mathbf{T}_{\zeta_{15}} + b_2\mathbf{T}_{\zeta_{15}^2} + b_4\mathbf{T}_{\zeta_{15}^4} + b_7\mathbf{T}_{\zeta_{15}^7} + b_8\mathbf{T}_{\zeta_{15}^8} + b_{11}\mathbf{T}_{\zeta_{15}^{11}} + b_{13}\mathbf{T}_{\zeta_{15}^{13}} + b_{14}\mathbf{T}_{\zeta_{15}^{14}},$$

where matrices $\mathbf{T}_{\zeta_{15}^i}$ respond to the elements of the integral normal basis $\zeta_{15}^i \in N$. Then it is useful have this matrices:

$$\mathbf{T}_{\zeta_{15}} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & -1 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & -1 & -1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & -1 & 0 & 1 & 1 \end{pmatrix}, \quad \mathbf{T}_{\zeta_{15}^2} = \begin{pmatrix} 0 & 0 & -1 & 0 & -1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 & -1 & 1 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 1 & 0 \end{pmatrix},$$

$$\mathbf{T}_{\zeta_{15}^4} = \begin{pmatrix} 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 & -1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 & 1 & 0 & -1 \\ -1 & -1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \\ -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \quad \mathbf{T}_{\zeta_{15}^7} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & -1 & -1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 1 & 1 & 0 & -1 & 0 \end{pmatrix},$$

$$\mathbf{T}_{\zeta_{15}^8} = \begin{pmatrix} 0 & -1 & 0 & 1 & 1 & 0 & -1 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ -1 & -1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & -1 & -1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad \mathbf{T}_{\zeta_{15}^{11}} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 \\ -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & -1 & -1 \\ -1 & 0 & 1 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & -1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \end{pmatrix},$$

$$
\begin{pmatrix}
a_{14} & -a_4-a_8+a_{13}+a_{14} & -a_2+a_{11} & a_8-a_{14} & -a_2+a_7+a_8-a_{13} & a_4-a_{14} & a_2-a_8 & a_1+a_2-a_7-a_{11} \\
a_1-a_4-a_{11}+a_{14} & a_{13} & -a_1-a_8+a_{11}+a_{13} & a_8-a_{13} & -a_4+a_7 & -a_1+a_4 & a_2+a_4-a_7-a_{14} & a_1-a_{13} \\
-a_8+a_{14} & a_2-a_7-a_8+a_{13} & a_{11} & -a_2+a_8 & -a_1-a_2+a_7+a_{11} & a_4+a_8-a_{13}-a_{14} & a_2-a_{11} & a_1-a_{11} \\
-a_{11}+a_{14} & -a_8+a_{13} & -a_8+a_{11} & a_8 & -a_2-a_4+a_7+a_{14} & -a_1+a_4+a_{11}-a_{14} & a_2-a_{14} & a_1+a_8-a_{11}-a_{13} \\
-a_2-a_4+a_7+a_{14} & -a_1+a_{13} & -a_1+a_4+a_{11}-a_{14} & a_1+a_8-a_{11}-a_{13} & a_7 & a_4-a_7 & a_2-a_7 & a_1-a_4 \\
-a_4+a_{14} & -a_4+a_{13} & -a_1-a_2+a_7+a_{11} & a_4+a_8-a_{13}-a_{14} & a_7-a_{13} & a_4 & a_2-a_7-a_8+a_{13} & a_1-a_7 \\
-a_2+a_{14} & -a_1-a_8+a_{11}+a_{13} & a_{11}-a_{14} & a_8-a_{11} & -a_2+a_7 & a_2+a_4-a_7-a_{14} & a_2 & a_1-a_4-a_{11}+a_{14} \\
-a_4-a_8+a_{13}+a_{14} & -a_7+a_{13} & -a_1+a_{11} & -a_2+a_7+a_8-a_{13} & -a_1+a_7 & a_4-a_{13} & a_1+a_2-a_7-a_{11} & a_1
\end{pmatrix}
$$

Figure 1: Matrix $\mathbf{T}_\alpha$.

$$\mathbf{T}_{\zeta_{15}^{13}} = \begin{pmatrix} 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 1 & -1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & -1 & 0 & -1 & 0 & 0 \end{pmatrix}, \quad \mathbf{T}_{\zeta_{15}^{14}} = \begin{pmatrix} 1 & 1 & 0 & -1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & -1 & -1 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & -1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

Let $K \subseteq \mathbb{Q}(\zeta_{15})$ is the unique quadratic field with the conductor 15. Then the elements of integral normal basis of K are

$$\varepsilon_1 = \zeta_{15} + \zeta_{15}^2 + \zeta_{15}^4 + \zeta_{15}^8,$$
$$\varepsilon_2 = \zeta_{15}^7 + \zeta_{15}^{14} + \zeta_{15}^{13} + \zeta_{15}^{11}.$$

We found matrices $\mathbf{T}_{\varepsilon_1}$ and $\mathbf{T}_{\varepsilon_2}$,

$$\mathbf{T}_{\varepsilon_1} = \begin{pmatrix} 0 & -2 & -1 & 1 & 0 & 1 & 0 & 2 \\ 0 & 0 & -2 & 1 & -1 & 0 & 2 & 1 \\ -1 & 0 & 0 & 0 & -2 & 2 & 1 & 1 \\ 0 & -1 & -1 & 1 & -2 & 0 & 1 & 2 \\ -2 & -1 & 0 & 2 & 0 & 1 & 1 & 0 \\ -1 & -1 & -2 & 2 & 0 & 1 & 0 & 1 \\ -1 & -2 & 0 & 1 & -1 & 2 & 1 & 0 \\ -2 & 0 & -1 & 0 & -1 & 1 & 2 & 1 \end{pmatrix}, \quad \mathbf{T}_{\varepsilon_2} = \begin{pmatrix} 1 & 2 & 1 & -1 & 0 & -1 & 0 & -2 \\ 0 & 1 & 2 & -1 & 1 & 0 & -2 & -1 \\ 1 & 0 & 1 & 0 & 2 & -2 & -1 & -1 \\ 0 & 1 & 1 & 0 & 2 & 0 & -1 & -2 \\ 2 & 1 & 0 & -2 & 1 & -1 & -1 & 0 \\ 1 & 1 & 2 & -2 & 0 & 0 & 0 & -1 \\ 1 & 2 & 0 & -1 & 1 & -2 & 0 & 0 \\ 2 & 0 & 1 & 0 & 1 & -1 & -2 & 0 \end{pmatrix}.$$

Now the representatives of ε_1 a ε_2 regarding to subfield K are

$$\mathbf{T}_{\varepsilon_1,K} = \begin{pmatrix} -3 & 4 \\ -4 & 4 \end{pmatrix}, \quad \mathbf{T}_{\varepsilon_2,K} = \begin{pmatrix} 4 & -4 \\ 4 & -3 \end{pmatrix}.$$

Let $\alpha \in K$, such that $\alpha = a\varepsilon_1 + b\varepsilon_2$, then

$$\mathbf{T}_{\alpha,K} = \begin{pmatrix} -3a + 4b & 4a - 4b \\ -4a + 4b & 4a - 3b \end{pmatrix}.$$

Trace and norm of α are

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\alpha) = a + b,$$
$$\mathrm{N}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\alpha) = -27a^2 + 25ab - 27b^2.$$

References

[1] Borevich, Z. I, Shafarevich, I. R., *Number Theory*, Moscow, 1964.

[2] Davis, P., J., *Circulant matrices*, J. Wiley & Sons, Inc., New York, 1979.

[3] Jakubec, S., Kostra, J., Nemoga, K., *On the existence of an integral normal basis generated by a unit in prime extensions of rational numbers*, Mathematics of computation **56** (1991), no. 194, 809–815.

[4] Jakubec, S., Kostra, J., *A note on normal bases of ideals*, Math. Slovaca **42** (1992), no. 5, 677–684.

[5] Jakubec, S., Kostra, J., *On the Existence of a Normal Basis for an Ambiguous Ideal*, Atti Sem. Mat. Fis. Univ. Modena **XLVI** (1998), 125–129.

[6] Kostra, J., *A Note on Representation of Cyclotomic Fields*, Acta Math. Inf. Univ. Ostraviensis **4** (1996), 29—35.

Author's address: Department of Mathematics, Faculty of Science, University of Ostrava, Bráfova 7, 701 03 Ostrava, Czech republic.

Institute of Mathematics, VŠB–TU, 17. Listopadu 15, 708 33 Ostrava-Poruba, Czech republic.

E-mail: marek.pomp@osu.cz

radim.havelek@vsb.cz

Received: January 15, 1999