VERSITA

Mathematica Slovaca

DOI: 10.2478/s12175-012-0082-1
Math. Slovaca **63** (2013), No. 1, 63–68

PROPERTIES OF TRANSFORMATION MATRICES BETWEEN THE NORMAL BASES IN ORDERS OF CUBIC FIELD

Zuzana Divišová-Václavíková

(*Communicated by Stanislav Jakubec*)

ABSTRACT. In this paper, the properties of transformation matrices between the normal bases in orders of algebraic number fields of degree 3 are shown.

Let K be a finite extension of the rational number field $\mathbb{Q}$ and let the $\mathbb{Z}_K$ be integral closure of the ring $\mathbb{Z}$ in K — i.e. the ring of integral numbers of the field K.

Definition 1. Let K be an algebraic number field of degree n over the rational numbers $\mathbb{Q}$. A $\mathbb{Z}$-module $B \subset K$ is called an *order of the field* K if B satisfies the following conditions:

(1) $1 \in B$,
(2) B has a basis over $\mathbb{Z}$ consisting of n elements,
(3) B is ring.

Let K be a cyclic algebraic number field of degree n over $\mathbb{Q}$. Such a field has a normal basis over $\mathbb{Q}$, i.e. a basis which consists of all conjugations of one element.

Transformation matrices between two normal bases of K over $\mathbb{Q}$ are exactly regular rational circulant matrices of degree n.

In [5] Kostra characterized the special class of circulant matrices with rational integral elements by:

2010 Mathematics Subject Classification: Primary 11R33; Secondary 11C20.
Keywords: Circulant matrix, order, normal basis.

Theorem 1. *Let K be cyclic algebraic number field of degree n over $\mathbb{Q}$. Let*

$$A = \operatorname{circ}_n(a_1, a_2, \dots, a_n)^T$$

be a circulant matrix and $a_i \in \mathbb{Z}$ for all i. By A_i for $i = 1, 2, \dots, n$ we denote the algebraic complement of a_i in the matrix A. Let

(1) $a_1 + a_2 + \cdots + a_n = \pm 1$ *and*
(2) $a_i \equiv a_j \pmod{h}$ *for all $i, j \in \{1, 2, \dots, n\}$ where* $h = \frac{\det A}{\gcd(A_1, \dots, A_n)}$

Then the matrix A transform a normal basis of an order B of the field K to a normal basis of an order C where $C \subseteq B$.

In [3] the matrices satisfying the Theorem 1 have been characterized as follows:

Theorem 2. *Let G be a multiplicative semigroup of circulant matrices of degree n satisfying the assumptions of the* Theorem 1. *Let U be multiplicative group of unimodular circulant matrices of degree n. Let H be the semigroup of circulant matrices of the type* $\operatorname{circ}_n(a, b, \dots, b)$ *such that $a+(n-1)b = \pm 1$. Then $G = H \cdot U$.*

In this paper, the properties of such transformation matrices between the normal bases in orders of algebraic number fields of degree 3 are shown.

Theorem 3. *Let $A = \operatorname{circ}_3(a, b, c)$ be a circulant matrix over $\mathbb{Z}$ such that $a+b+c = \pm 1$. Then $a \equiv b \equiv c \pmod{\gcd(A_1, A_2, A_3)}$ and $\gcd(A_1, A_2, A_3)$ is the largest such number.*

Proof. Let A_i be an algebraic complement of element a_i in the matrix A. So $A_1 = a^2 - bc$, $A_2 = b^2 - ac$ and $A_3 = c^2 - ab$. Let us denote $\gcd(A_1, A_2, A_3) = g$. We can write

$$A_1 - A_2 = a^2 - bc - b^2 + ac = (a - b)(a + b + c)$$

and because $\gcd(A_1, A_2, A_3) = g$ then $g \mid A_1$ and $g \mid A_2$ so $g \mid (A_1 - A_2)$ and with respect that $a + b + c = \pm 1$ it follows $g \mid (a - b)$, i.e. $a \equiv b \mod g$.

Analogously,

$$A_2 - A_3 = (b - c)(a + b + c)$$

so $g \mid (b - c)$ and we can write $a \equiv b \equiv c \pmod{g}$.

On the other hand, let us suppose that $a \equiv b \equiv c \pmod{g^\star}$. Then $a^2 \equiv bc \pmod{g^\star}$ and so $g^\star \mid A_1$. Analogously, $g^\star \mid A_2$ and $g^\star \mid A_3$. Because the $\gcd(A_1, A_2, A_3) = g$ then $g^\star \mid g$. □

Recall. Let ζ_n be the n-th primitive root of unity and denote by $\mathbb{Z}[\zeta_n]$ the ring of integers of n-th cyclotomic field. Let

$$A = \mathrm{circ}_n(a_1, a_2, \ldots, a_n)$$

be the circulant matrix of degree n. It is known (see for example [1]) that the eigenvalues of A are exactly

$$\lambda_j = p_\gamma(\zeta_n^{j-1})$$

for $j = 1, 2, \ldots, n$, where $p_\gamma(z) := a_1 + a_2 z + \cdots + a_n z^{n-1}$ is the polynomial corresponding to $\gamma = (a_1, a_2, \ldots, a_n)$.

In this case we have $n = 3$ so the eigenvalues of the circulant matrix $A = \mathrm{circ}_3(a, b, c)$ are

$$\lambda_j = p_\gamma(\zeta_3^{j-1})$$

for $j = 1, 2, 3$ where $p_\gamma(z) := a + bz + cz^2$ is the polynomial corresponding to $\gamma = (a, b, c)$ and the ζ_3 is the primitive third root of unity. So

$$\lambda_1 = a + b\zeta_3^0 + c\zeta_3^0 = a + b + c,$$

i.e. sum of the first row, and using the fact $1 + \zeta_3 + \zeta_3^2 = 0$ we have

$$\lambda_2 = a + b\zeta_3 + c\zeta_3^2 = (a - c) + (b - c)\zeta_3$$

and

$$\lambda_3 = a + b\zeta_3^2 + c\zeta_3^4 = (a - b) + (c - b)\zeta_3.$$

Theorem 4. *Let $A = \mathrm{circ}_3(a, b, c)$ be a circulant matrix over $\mathbb{Z}$ such that $a+b+c = \pm 1$. Let $g \in \mathbb{N}$ be the largest such number that $a \equiv b \equiv c \pmod{g}$. Then g is the largest such that $g \mid \lambda_2$ and $g \mid \lambda_3$ where $\lambda_2 = a+b\zeta_3+c\zeta_3^2$, $\lambda_3 = a+b\zeta_3^2+c\zeta_3$ are the eigenvalues of the matrix A.*

Proof. Let $A = \mathrm{circ}_3(a, b, c)$ such that $a + b + c = \pm 1$. The eigenvalues of the circulant matrix A are $\lambda_1 = a + b + c$, $\lambda_2 = a + b\zeta_3 + c\zeta_3^2 = (a - c) + (b - c)\zeta_3$ and $\lambda_3 = a + b\zeta_3^2 + c\zeta_3^4 = (a - b) + (c - b)\zeta_3$.

Let $a \equiv b \equiv c \pmod{g}$. Then $g \mid (a - b)$, $g \mid (a - c)$ and $g \mid (b - c)$ so $g \mid \lambda_2$ and $g \mid \lambda_3$.

Let us suppose that for some $g^\star \in \mathbb{N}$ we have $g^\star \mid \lambda_2$ and $g^\star \mid \lambda_3$. Because $1, \zeta$ are linearly independent over the $\mathbb{Z}$, it follows $g^\star \mid (a - c)$, $g^\star \mid (b - c)$ and so $a \equiv b \equiv c \pmod{g^\star}$. Using the fact, that g was the largest such number we get $g^\star \mid g$. $\square$

Theorem 5. *Let $A = \mathrm{circ}_3(a, b, c)$ be a circulant matrix over $\mathbb{Z}$ such that $a+b+c = \pm 1$. Then the eigenvalues λ_2 and λ_3 are associated in $\mathbb{Z}[\zeta_3]$, if and only if $a = b$ or $b = c$ or $a = c$.*

P r o o f.

$\Longleftarrow$ is trivial. If $a = b$ then $\lambda_2 = (a - c) + (b - c)\zeta_3 = (b - c)(1 + \zeta_3) = (b - c)(-\zeta_3^2)$ and $\lambda_3 = (a - b) + (c - b)\zeta_3 = (c - b)\zeta_3$ so the λ_2 and λ_3 are associated in $\mathbb{Z}[\zeta_3]$ because the $\zeta_3, -\zeta_3^2$ are the units. Analogously for $b = c$ and $a = c$.

$\Longrightarrow$: Let λ_2 and λ_3 are associated in $\mathbb{Z}[\zeta_3]$. Then there exists a unit $u \in \mathbb{Z}[\zeta_3]$ such that $\lambda_3 = u\lambda_2$. We know that units in $\mathbb{Z}[\zeta_3]$ are $u = \pm\zeta_3^k$ where $k = 0, 1, 2$ so we get

$$\lambda_3 = (a - b) + (c - b)\zeta_3 = \pm\zeta_3^k((a - c) + (b - c)\zeta_3) = \pm\zeta_3^k\lambda_2$$

for $k = 0, 1, 2$. For $k = 0$ we obtain $(a - b) + (c - b)\zeta_3 = (a - c) + (b - c)\zeta_3$ or $(a - b) + (c - b)\zeta_3 = -((a - c) + (b - c)\zeta_3)$ so

$$a - b = a - c, c - b = b - c$$

which implies $b = c$ or

$$a - b = c - a, c - b = c - b$$

which implies no solution in $\mathbb{Z}$ because $a + b + c = \pm 1$.

Analogously, the case $k = 1$ implies $a = c$ and the case $k = 2$ implies $a = b$. $\square$

With regard to the Theorem 1 and Theorem 2 we can deduce the corollary of the properties described in Theorems 3, 4 and 5 in the next example.

Example 1. Let $A = \mathrm{circ}_3(a, b, c)$ be a circulant matrix over $\mathbb{Z}$ with $a+b+c = 1$ such that $\det A = p^2$ where the p is a prime number. It is easy to calculate that $\det A = 1 - 3b - 3c + 3b^2 + 3c^2 + 3bc \equiv 1 \pmod 3$. So

(1) $p \equiv 2 \pmod 3$ or
(2) $p \equiv 1 \pmod 3$.

Because $\det A = \lambda_1\lambda_2\lambda_3$ and $\lambda_1 = a + b + c = 1$ we have $\det A = \lambda_2\lambda_3$.

In the case 1. if $p \equiv 2 \pmod 3$ then $p^2 \equiv 1 \pmod 3$ so $p\mathbb{Z}[\zeta_3] = \mathfrak{p}$. We get $\lambda_2 = a + b\zeta + c\zeta^2 = u_1p$ and $\lambda_3 = a + b\zeta^2 + c\zeta = u_2p$ where u_1, u_2 are the units in $\mathbb{Z}[\zeta_3]$. The eigenvalues satisfy the assumptions of Theorem 5 and with respect to the Theorems 1,2 the matrix transforms a normal basis of the order to a normal basis of its suborder in a cyclic algebraic number field of degree 3.

In the case 2. if $p \equiv 1 \pmod 3$ then $p\mathbb{Z}[\zeta_3] = \mathfrak{P}_1\mathfrak{P}_2$ so there will exist two types of matrices.

The first type are such matrices that $\lambda_2 = u_1\mathfrak{P}_1\mathfrak{P}_2$ and $\lambda_3 = u_2\mathfrak{P}_1\mathfrak{P}_2$ where u_1, u_2 the units in $\mathbb{Z}[\zeta_3]$ which satisfy the assumptions of Theorem 5 and so transforms a normal basis of the order to a normal basis of its suborder in a cyclic algebraic number field of degree 3.

For example if we take the cubic cyclic algebraic number field $\mathbb{Q}[\zeta_7 + \zeta_7^{-1}]$, i.e. maximal real subfield of $\mathbb{Q}[\zeta_7]$, the order $\mathbb{Z}[\zeta_7 + \zeta_7^{-1}]$ with normal basis $\{\zeta_7 + \zeta_7^{-1}, \zeta_7^2 + \zeta_7^{-2}, \zeta_7^3 + \zeta_7^{-3}\}$, then the matrix $A = \operatorname{circ}_3(9, -4, -4)$ has $\det A = 13^2$ and the eigenvalues are $\lambda_2 = 13, \lambda_3 = 13$. Such matrix satisfies the assumptions of the Theorems 1,2 so it transforms a normal basis of any order to the normal basis of its suborder in cyclic algebraic number field.

The second type are the matrices with $\lambda_2 = u_1\mathfrak{P}_1^2$ and $\lambda_3 = u_2\mathfrak{P}_2^2$. Such a matrix does not satisfy the assumptions of Theorem 5, so there could exists a basis of order of cyclic cubic algebraic number field which will not be transformed by this matrix to a normal basis of its suborder.

If we take again the cubic cyclic algebraic number field $\mathbb{Q}[\zeta_7 + \zeta_7^{-1}]$, the order $\mathbb{Z}[\zeta_7 + \zeta_7^{-1}]$ with normal basis

$$\{\zeta_7 + \zeta_7^{-1}, \zeta_7^2 + \zeta_7^{-2}, \zeta_7^3 + \zeta_7^{-3}\} \tag{1}$$

and the matrix $B = \operatorname{circ}_3(-7, 8, 0)$ with $\det B = \det A = 13^2$. The eigenvalues of B are $\lambda_2 = -7 + 8\zeta_3$ and $\lambda_3 = -15 - 8\zeta_3$ which are not associated in $\mathbb{Z}[\zeta_3]$.

Let us transform the basis (1) by the circulant matrix $B = \operatorname{circ}_3(-7, 8, 0)$. We obtain a new basis

$$\begin{aligned}\big\{-7(\zeta_7 + \zeta_7^{-1}) + 8(\zeta_7^2 + \zeta_7^{-2}), -7(\zeta_7^2 + \zeta_7^{-2}) + 8(\zeta_7^3 + \zeta_7^{-3}),&\\ 8(\zeta_7 + \zeta_7^{-1}) - 7(\zeta_7^3 + \zeta_7^{-3})\big\}.&\end{aligned} \tag{2}$$

The $\mathbb{Z}$-module generated by this new basis (2) is not a ring, because it is not closed under the multiplication. For example the square of the first basis element is equal to

$$\begin{aligned}(-7(\zeta_7 + \zeta_7^{-1}) + 8(\zeta_7^2 + \zeta_7^{-2}))^2 = &-\frac{43234}{13^2}(-7(\zeta_7 + \zeta_7^{-1}) + 8(\zeta_7^2 + \zeta_7^{-2}))\\ &-\frac{45137}{13^2}(-7(\zeta_7^2 + \zeta_7^{-2}) + 8(\zeta_7^3 + \zeta_7^{-3}))\\ &-\frac{44970}{13^2}(8(\zeta_7 + \zeta_7^{-1}) - 7(\zeta_7^3 + \zeta_7^{-3})),\end{aligned}$$

so the coefficients are not integers, i.e. this element does not belong to the $\mathbb{Z}$-module generated by the new basis (2).

This matrix does not satisfy the assumption of Theorem 1 and will transform the basis of order to a basis of the structure which will not be closed as a ring, so it will not be a basis of suborder.

REFERENCES

[1] DAVIS, P. J.: *Circulant Matrices*, A. Wiley-Interscience publisher, John Wiley and Sons, New York-Chichester-Brisbane-Toronto, 1979.

[2] DIVIŠOVÁ, Z.—KOSTRA, J.—POMP, M.: *On transformation matrices connected to normal bases in cubic fields*, Acta Acad. Paedagog. Agriensis Sect. Mat. (N.S.) **29** (2002), 61–66.

[3] DIVIŠOVÁ, Z.—KOSTRA, J.—POMP, M.: *On transformation matrices connected to normal bases in orders*, JP J. Algebra Number Theory Appl. **3** (2003), 43–52.

[4] KOSTRA, J.: *On correspondence between orders and ideals with normal basis in cyclic subfields of* $\mathbb{Q}(\zeta_p)$ *of prime degree* l, Math. Slovaca **60** (2010), 787–792.

[5] KOSTRA, J.: *Orders with a normal basis*, Czechoslovak Math. J. **35** (1985), 391–404.

[6] NEWMAN, M.: *Integral Matrices*, Academic Press, New York-London, 1972

Received 21. 7. 2010
Accepted 15. 12. 2010

Department of Mathematics
Faculty of Science
University of Ostrava
30. dubna 22
Ostrava
CZECH REPUBLIC
E-mail: zuzana.vaclavikova@osu.cz