Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **31** *(2004) 45–51*

ON TRANSFORMATION MATRICES CONNECTED TO NORMAL BASES IN RINGS

J. Kostra (Žilina, Slovakia), M. Vavroš (Ostrava, Czech Republic)

Abstract. In the paper [6, Problem 7] there is presented an open problem to characterize all circulant matrices which transform any normal basis of any order of cyclic algebraic number field K to a normal basis of its suborder in K. A conjecture is that if a circulant matrix $\mathbf{A}=\mathrm{circ}_n(a_1,a_2,\dots,a_n)$, $\sum_{i=1}^{n} a_i=\pm 1$, transforms some normal basis of ring to normal basis of its subring then it transforms any normal basis of ring to normal basis of its subring. In this paper it is shown that if $\sum_{i=1}^{n} a_i \neq \pm 1$, then the related conjecture is false.

AMS Classification Number: 11R16, 11C20

1. Introduction

Let K be a tamely ramified cyclic algebraic number field of degree n over the rational numbers $\mathbb{Q}$. It seems that $K \subset \mathbb{Q}(\zeta_m)$, where ζ_m is a m-th primitive root of unity and m is square free. Such a field has a normal basis over the rationals $\mathbb{Q}$, i.e. a basis consisting 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 the paper [6, Problem 7] there is presented an open problem to characterize all circulant matrices which transform any normal basis of any order of cyclic algebraic number field K to a normal basis of its suborder in K. A conjecture is that if a circulant matrix $\mathbf{A} = \mathrm{circ}_n(a_1, a_2, \dots, a_n)$, $\sum_{i=1}^{n} a_i = \pm 1$, transforms some normal basis of ring to a normal basis of its subring, then it transforms any normal basis of ring to a normal basis of its subring. In the paper it is shown that if $\sum_{i=1}^{n} a_i \neq \pm 1$, then the related conjecture is false.

In the paper [5], the special class of circulant matrices with integral rational elements is characterized by the following proposition.

This research was supported by VEGA 2/4138/24

Proposition 1. *Let K be a cyclic algebraic number field of degree n over rational numbers. Let*

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

be a circulant matrix and $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. By A_i, $i = 1, 2, \ldots n$ we denote the algebraic complement of element a_i in the matrix $\mathbf{A}$. Let

$$a_1 + a_2 + \cdots + a_n = \pm 1$$

and

$$a_i \equiv a_j \pmod{h}$$

for $i, j \in \{1, 2, \ldots, n\}$, where

$$h = \frac{\det \mathbf{A}}{\gcd(A_1, A_2, \ldots, A_n)}\,.$$

Then the matrix $\mathbf{A}$ transforms a normal basis of an order B of the field K to a normal basis of an order C of the field K, where $C \subseteq B$.

In the papers [3, 4] previous matrices are characterized by Theorem 3 [4].

Proposition 2. *Let G be a multiplicative semigroup of circulant matrices of degree n, satisfying the assumptions of Proposition 1. Let U be multiplicative group of integral unimodular circulant matrices of degree n. Let H be the semigroup of circulant matrices of type $\mathrm{circ}_n(a, b, \ldots, b)$, such that*

$$a + (n-1)b = \pm 1.$$

Then $G = H \cdot U$.

2. Results

First we recall the definition of order of algebraic number field.

Definition 1. Let K be an algebraic number field and let the degree of the extension $K/\mathbb{Q}$ be equal to n. A $\mathbb{Z}$-module $B \subset K$ is called an order of the field K if it satisfies the following conditions:

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

Remark 1. Matrices from Proposition 1 transform also normal bases rings which have a basis over $\mathbb{Z}$ consisting of n elements to normal bases of their subrings. Such rings we will call semiorders.

Definition 2. Let K be an algebraic number field and let the degree of the extension $K/\mathbb{Q}$ be equal to n. A $\mathbb{Z}$-module $B \subset K$ is called a semiorder of the field K if it satisfies the following conditions:

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

In the following it will be shown that the condition

$$a + (n-1)b = \pm 1.$$

from Proposition 1 for matrix $\mathrm{circ}_n(a, b, \ldots, b)$ is necessary.

Example 1. Let ζ_7 be a 7-th primitive root of unity and let $\langle \varepsilon_1, \varepsilon_2, \varepsilon_3 \rangle$ be a normal integral basis of the field $K = \mathbb{Q}^+(\zeta_7)$ over $\mathbb{Q}$, where

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

Let $\mathbf{A} = \mathrm{circ}_3(0, 5, 5)$ and $\langle \alpha_1, \alpha_2, \alpha_3 \rangle = \langle \varepsilon_1, \varepsilon_2, \varepsilon_3 \rangle \cdot \mathbf{A}$, so

$$\begin{aligned} \alpha_1 &= 5\varepsilon_2 + 5\varepsilon_3\,, \\ \alpha_2 &= 5\varepsilon_1 + 5\varepsilon_3\,, \\ \alpha_3 &= 5\varepsilon_1 + 5\varepsilon_2\,. \end{aligned}$$

Then

$$\alpha_1 \cdot \alpha_2 = \frac{-5}{2}\alpha_1 + \frac{5}{2}\alpha_2 + \frac{5}{2}\alpha_3$$

and the module $\mathbb{Z}[\alpha_1, \alpha_2, \alpha_3]$ is not a ring, so $\mathbb{Z}[\alpha_1, \alpha_2, \alpha_3]$ is not a semiorder.

Example 2. Let $\varepsilon_1, \varepsilon_3, \varepsilon_3$ and $\mathbf{A}$ be the same as in above example.

Let

$$\begin{aligned} \alpha_1 &= 2\varepsilon_1\,, \\ \alpha_2 &= 2\varepsilon_2\,, \\ \alpha_3 &= 2\varepsilon_3\,. \end{aligned}$$

and $\langle \beta_1, \beta_2, \beta_3 \rangle = \langle \alpha_1, \alpha_2, \alpha_3 \rangle \cdot \mathbf{A}$, so

$$\begin{aligned} \beta_1 &= 5\alpha_2 + 5\alpha_3\,, \\ \beta_2 &= 5\alpha_1 + 5\alpha_3\,, \\ \beta_3 &= 5\alpha_1 + 5\alpha_2\,. \end{aligned}$$

Then

$$\begin{aligned} \beta_1^2 &= -50\alpha_1 - 100\alpha_2 - 150\alpha_3\,, \\ \beta_2^2 &= -150\alpha_1 - 50\alpha_2 - 100\alpha_3\,, \\ \beta_3^2 &= -100\alpha_1 - 150\alpha_2 - 50\alpha_3\,. \end{aligned}$$

and

$$\beta_1 \cdot \beta_2 = 50\alpha_1\,,$$
$$\beta_2 \cdot \beta_3 = 50\alpha_2\,,$$
$$\beta_3 \cdot \beta_1 = 50\alpha_3\,.$$

We have

$$\beta_1^2 = -20\beta_1 - 10\beta_2\,,$$
$$\beta_2^2 = -20\beta_2 - 10\beta_3\,,$$
$$\beta_3^2 = -10\beta_1 - 20\beta_3\,.$$

and

$$\beta_1 \cdot \beta_2 = -5\beta_1 + 5\beta_2 + 5\beta_3\,,$$
$$\beta_2 \cdot \beta_3 = 5\beta_1 - 5\beta_2 + 5\beta_3\,,$$
$$\beta_3 \cdot \beta_1 = 5\beta_1 + 5\beta_2 - 5\beta_3\,.$$

And so $\mathbb{Z}[\alpha_1, \alpha_2, \alpha_3]$ is a semiorder.

By the previous examples we have that in the case $\mathbf{A} = \mathrm{circ}_n(a_1, a_2, \ldots, a_n)$, $\sum_{i=1}^{n} a_i \neq \pm 1$, the conjecture from [6], that if a circulant matrix transforms some normal basis of a semiorder to normal basis of its subsemiorder then it transforms any normal basis of any semiorder to normal basis of its subsemiorder, does not hold.

Theorem 1. *Let $\mathbf{A}' = \mathrm{circ}_n(a, b, \ldots, b)$, $a + (n-1)b = 1$. Let $\mathbf{A} = \mathrm{circ}_n(0, b-a, \ldots, b-a)$. Let $b \equiv 1 \pmod{n-1}$, then matrix $\mathbf{A} \cdot \mathbf{U}$, where $\mathbf{U}$ is a unimodular circulant matrix of degree n, transforms any normal basis of any semiorder R to a normal basis of its subsemiorder S.*

Proof. Let $\mathbf{A}' = \mathrm{circ}_n(a, b, \ldots, b)$, $a + (n-1)b = 1$, $\mathbf{A} = \mathrm{circ}_n(0, b-a, \ldots, b-a)$ and $b \equiv 1 \pmod{n-1}$. From

$$a + (n-1)b = 1$$

we obtain

$$b - a = nb - 1.$$

So

$$\det \mathbf{A} = (-1)^{n-1} \cdot (n-1) \cdot (nb-1)^n.$$

Then

$$\mathbf{A^{-1}} = \mathrm{circ}_n\left(-\frac{n-2}{(n-1)\cdot(nb-1)}, \frac{1}{(n-1)\cdot(nb-1)}, \ldots, \frac{1}{(n-1)\cdot(nb-1)}\right).$$

Let $\langle\alpha_1,\alpha_2,\dots,\alpha_n\rangle$ be a normal basis of semiorder R. Let

$$\langle\beta_1,\beta_2,\dots,\beta_n\rangle = \langle\alpha_1,\alpha_2,\dots,\alpha_n\rangle\cdot\mathbf{A}$$

be a normal basis of submodule $S\subset R$. Then

$$\begin{aligned}
\beta_1 &= (nb-1)\alpha_2 + (nb-1)\alpha_3 + \cdots + (nb-1)\alpha_n\,,\\
\beta_2 &= (nb-1)\alpha_1 + (nb-1)\alpha_3 + \cdots + (nb-1)\alpha_n\,,\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
\beta_n &= (nb-1)\alpha_1 + (nb-1)\alpha_2 + \cdots + (nb-1)\alpha_{n-1}\,.
\end{aligned}$$

From the above it follows that for all i,j

$$\beta_i\beta_j = (nb-1)^2\cdot(b_1\alpha_1 + b_2\alpha_2 + \cdots + b_n\alpha_n),$$

where $b_i\in\mathbb{Z}$ for all i. By the expression of $\mathbf{A^{-1}}$ we have for any i,j

$$\beta_i\beta_j = c_1\beta_1 + \cdots + c_n\beta_n$$

$$= \frac{(nb-1)}{(n-1)}\cdot(d_1\beta_1 + \cdots + d_n\beta_n).$$

If $b\equiv 1 \pmod{n-1}$, then coefficients $c_i\in\mathbb{Z}$, and S is a subsemiorder of the semiorder R. Clearly the same holds for $\mathbf{A}\cdot\mathbf{U}$, where $\mathbf{U}$ is a unimodular circulant matrix of degree n.

Remark 2. Matrix $\mathbf{A}=\mathrm{circ}_3(0,5,5)$ from Examples 1, 2 was obtained from matrix $\mathbf{A}'=\mathrm{circ}_3(-3,2,2)$ and $2\not\equiv 1 \pmod 2$.

Remark 3. If in the above Theorem 1 $a+(n-1)b=-1$, then if $b\equiv -1 \pmod{n-1}$ matrix $\mathbf{A}$ transforms a normal basis of any semiorder R to a normal basis of subsemiorder $S\subset R$.

The previous Theorem 1 gives the way to find a circulant matrix $\mathbf{A}$ of arbitrary degree for which there exist semiorders R_1,R_2 such that $\mathbf{A}$ transforms a normal basis of R_i to a normal basis of submodule $S_i\subset R_i$ and S_1 is a semiorder and S_2 is not a ring and so S_2 is not a semiorder.

Example 3. Let ζ_{11} be an 11-th primitive root of units and let $\langle\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_4,\varepsilon_5\rangle$, where

$$\varepsilon_1=\zeta_{11}+\zeta_{11}^{10},\ \varepsilon_2=\zeta_{11}^{2}+\zeta_{11}^{9},\ \varepsilon_3=\zeta_{11}^{3}+\zeta_{11}^{8},\ \varepsilon_4=\zeta_{11}^{4}+\zeta_{11}^{7},\ \varepsilon_5=\zeta_{11}^{5}+\zeta_{11}^{6},$$

be a normal integral basis of the field $K=\mathbb{Q}^+(\zeta_{11})$ over $\mathbb{Q}$. The field $K=\mathbb{Q}(\zeta_{11}+\zeta_{11}^{-1})$ is the maximal real subfield of $\mathbb{Q}(\zeta_{11})$.

Let $\mathbf{A}'=\mathrm{circ}_5(a,b,b,b,b)=\mathrm{circ}_5(-7,2,2,2,2),\ a+4b=1,\ b\not\equiv 1 \pmod 4$. Let

$$\mathbf{A}=\mathrm{circ}_5(0,\ 5b-1,\ 5b-1,\ 5b-1,\ 5b-1)=\mathrm{circ}_5(0,9,9,9,9),$$

$$A^{-1} = circ_5\left(-\frac{1}{12}, \frac{1}{36}, \frac{1}{36}, \frac{1}{36}, \frac{1}{36}\right)$$

and $R_2 = \langle \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5 \rangle$, $S_2 = \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \rangle$, where

$$\langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \rangle = \langle \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5 \rangle \cdot \mathbf{A},$$

so

$$\begin{aligned}\alpha_1 &= 9\varepsilon_2 + 9\varepsilon_3 + 9\varepsilon_4 + 9\varepsilon_5\,,\\ \alpha_2 &= 9\varepsilon_1 + 9\varepsilon_3 + 9\varepsilon_4 + 9\varepsilon_5\,.\end{aligned}$$

Then

$$\alpha_1 \cdot \alpha_2 = 81\varepsilon_1 - 81\varepsilon_4 - 81\varepsilon_5.$$

After transformation by matrix $\mathbf{A}^{-1}$ we have

$$\alpha_1 \cdot \alpha_2 = -\frac{45}{4}\alpha_1 - \frac{9}{4}\alpha_2 - \frac{9}{4}\alpha_3 - \frac{81}{4}\alpha_4 - \frac{81}{4}\alpha_5.$$

From this it follows that S_2 is not a ring.

And now let $R_1 = \langle \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5 \rangle$ and $S_1 = \langle \beta_1, \beta_2, \beta_3, \beta_4, \beta_5 \rangle$, where

$$\begin{aligned}\beta_1 &= 6\varepsilon_1\,,\\ \beta_2 &= 6\varepsilon_2\,,\\ \beta_3 &= 6\varepsilon_3\,,\\ \beta_4 &= 6\varepsilon_4\,,\\ \beta_5 &= 6\varepsilon_5\,.\end{aligned}$$

$$\langle \gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5 \rangle = \langle \beta_1, \beta_2, \beta_3, \beta_4, \beta_5 \rangle \cdot \mathbf{A}$$

We have $\gamma_i\gamma_j = 36 \cdot (b_1\beta_1 + b_2\beta_2 + \cdots + b_5\beta_5)$. From the expression of $\mathbf{A}^{-1}$ it follows that $\gamma_i\gamma_j = c_1\gamma_1 + c_2\gamma_2 + \cdots + c_5\gamma_5$ with integral rational coefficients c_i. So S_1 is a semiorder.

References

[1] Borevich, Z. I., Shafarevich, I. R., *Number theory*, Nauka, Moscow, 1985. **3**rd ed. (in Russian).

[2] Davis, P. J., *Circulant matrices*, A. Wiley-Interscience Publisher, John Wiley and Sons, New York–Chichester–Brisbane–Toronto, 1979.

[3] Divišová, Z., Kostra, J., Pomp, M., On transformation matrices connected to normal bases in cubic fields, *Acta Acad. Paed. Agriensis, Sectio Mathematicae* **29** (2002), 61–66.

[4] Divišová, Z., Kostra, J., Pomp, M., On transformation matrix connected to normal bases in orders, *JP Jour. Algebra, Number Theory and Appl.* **3/1** (2003), 43–52.

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

[6] Kostra, J., Open problems on the relation between additive and multiplicative structure, *Annales Mathematicae Silesianae* **16** (2003), 21–25.

J. Kostra
Department of Algebra, Geometry and Didactics
University of Žilina
Hurbanova 15
Žilina, Slovak Republic
E-mail: juraj.kostra@fpv.utc.sk

M. Vavroš
Department of Mathematics
University of Ostrava
30. dubna 22
Ostrava, Czech Republic
E-mail: michal.vavros@osu.cz