Acta Acad. Paed. Agriensis, Sectio Mathematicae **29** *(2002) 61–66*

ON TRANSFORMATION MATRICES CONNECTED TO NORMAL BASES IN CUBIC FIELDS

Z. Divišová, J. Kostra, M. Pomp (Ostrava, Czech Republic)

Dedicated to the memory of Professor Péter Kiss

Abstract. In the paper it is proved that special class of circulant matrices transforming normal bases of orders in cubic fields to normal bases of their suborders consists of matrices of the type $\mathrm{circ}_3(a_1,a_2,a_3)$ where $a_1+a_2+a_3=\pm 1$ and one of the equalities $a_1=a_2$, $a_1=a_3$, $a_2=a_3$ holds.

AMS Classification Number: 11R16, 11C20

1. Introduction

Let K be a cyclic algebraic number field of degree n over the rational numbers $\mathbb{Q}$. 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 [4], the special class of circulant matrices with integral rational elements is characterized by the following proposition.

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

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

This research was supported by GA of the Czech Academy of Sciences Grant A1187101/01.

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* $C \subseteq B$*.*

2. Results

Theorem 1. *Let* $\mathbf{A}$ *be a circulant matrix* $\mathbf{A} = \mathrm{circ}_3(a_1, a_2, a_3)$*,* $a_i \in \mathbb{Z}$*, where*

$$a_1 + a_2 + a_3 = \pm 1.$$

Then the following conditions are equivalent

(1) $a_i \equiv a_j \pmod{h}$ *for* $i, j \in \{1, 2, 3\}$*, where*

$$h = \frac{\det \mathbf{A}}{\gcd(A_1, A_2, A_3)}\,,$$

where A_i *is algebraic complement of element* a_i *in the matrix* $\mathbf{A}$ *for every* $i \in \{1, 2, 3\}$*.*

(2) *One of the next equalities holds*

$$a_1 = a_2 \quad \text{or} \quad a_2 = a_3 \quad \text{or} \quad a_1 = a_3\,.$$

Proof. (1) $\Rightarrow$ (2) Let $\mathbf{A} = \mathrm{circ}_3(a_1, a_2, a_3)$ be a circulant matrix fulfilling assumptions of our theorem. If $a_1 + a_2 + a_3 = 1$, we can write

$$\mathbf{A} = (1 - a_2 - a_3, a_2, a_3)\,.$$

Determinant of the matrix $\mathbf{A}$ is

$$\begin{aligned} \det \mathbf{A} &= 1 + 3a_2^2 + 3a_3^2 - 3a_2 - 3a_3 + 3a_2a_3 \\ &= (1 - 3a_2)(1 - 3a_3) + 3(a_2 - a_3)^2 \end{aligned} \tag{1}$$

and the subdeterminants are

$$\begin{aligned} A_1 &= 1 + a_2^2 + a_3^2 - 2a_2 - 2a_3 + a_2a_3\,, \\ A_2 &= a_2^2 + a_3^2 + a_2a_3 - a_3\,, \\ A_3 &= a_2^2 + a_3^2 + a_2a_3 - a_2\,. \end{aligned}$$

Their greatest common divisor is

$$\begin{aligned}
&\gcd(A_1, A_2, A_3) = \gcd(A_1 - A_2, A_2, A_3 - A_2)\\
&= \gcd(1 - 2a_2 - a_3, a_2^2 + a_3^2 + a_2a_3 - a_3, a_3 - a_2)\\
&= \gcd\big(1 - 2a_2 - a_3 + (a_3 - a_2), a_2^2 + a_3^2 + a_2a_3 - a_3 + (a_2 + 2a_3)(a_3 - a_2), a_3 - a_2\big)\\
&= \gcd(1 - 3a_2, -a_3 + 3a_3^2, a_3 - a_2)\\
&= \gcd\big(1 - 3a_2, -a_3(1 - 3a_3), a_3 - a_2\big).
\end{aligned}$$

In regards with (1) we obtain that $\gcd(A_1, A_2, A_3)^2$ is a divisor of $\det \mathbf{A}$. Now we need to prove that $\det \mathbf{A}$ is a divisor of $\gcd(A_1, A_2, A_3)^2$.

Because of $a_i \equiv a_j \pmod h$ for $i, j \in \{1, 2, 3\}$, we obtain the congruences

$$\begin{aligned}
a_3 - a_2 &\equiv 0 \pmod h,\\
1 - 3a_2 &\equiv 0 \pmod h,\\
1 - 3a_3 &\equiv 0 \pmod h.
\end{aligned} \tag{2}$$

Then h is a divisor of $\gcd(A_1, A_2, A_3)$,

$$\begin{aligned}
\gcd(A_1, A_2, A_3) = kh &= k\frac{\det \mathbf{A}}{\gcd(A_1, A_2, A_3)}\,,\\
\gcd(A_1, A_2, A_3)^2 &= k \det \mathbf{A}\,,
\end{aligned}$$

and $\det \mathbf{A}$ is a divisor of $\gcd(A_1, A_2, A_3)^2$. Therefore

$$\det \mathbf{A} = \pm\gcd(A_1, A_2, A_3)^2$$

and

$$h = \gcd(A_1, A_2, A_3)\,.$$

In regards of (2) we denote

$$hX = 1 - 3a_2\,, \quad hY = 1 - 3a_3\,, \quad hZ = a_2 - a_3\,,$$

then

$$\det \mathbf{A} = h^2XY + 3h^2Z^2\,.$$

We obtain the equation $XY + 3Z^2 = \pm 1$. Assumption $a_1 + a_2 + a_3 = 1$ yields the equation $hX + 3hZ = hY$.

(a) Let $\det \mathbf{A} = -h^2$. From the system of equations

$$\begin{aligned}
XY + 3Z^2 &= -1\,,\\
X + 3Z &= Y\,,
\end{aligned}$$

we obtain the quadratic equation in Z

$$3Z^2 - 3ZY + (Y^2 + 1) = 0$$

which has a negative discriminant, so there is no integral solution.

(b) Let $\det \mathbf{A} = h^2$. We obtain a system of equations

$$\begin{aligned} XY + 3Z^2 &= 1\,, \\ X + 3Z &= Y\,. \end{aligned}$$

From the integral solutions of this system it follows that

(a) $X = 1$, $Y = 1$, $Z = 0$ or $X = -1$, $Y = -1$, $Z = 0$ then $a_2 = a_3$,

(b) $X = 1$, $Y = -2$, $Z = -1$ or $X = -1$, $Y = 2$, $Z = 1$ then $a_1 = a_2$,

(c) $X = 2$, $Y = -1$, $Z = -1$ or $X = -2$, $Y = 1$, $Z = 1$ then $a_1 = a_3$.

The case $a_1 + a_2 + a_3 = -1$ can be proved similarly.

(2) $\Rightarrow$ (1) Without loss of generality it is sufficient to suppose that $a_2 = a_3$, so we can denote the matrix $\mathbf{A} = \mathrm{circ}_3(a, b, b)$. The algebraic complements are $A_1 = (a-b)(a+b)$, $A_2 = A_3 = b(b-a)$ so the $\gcd(A_1, A_2, A_3) = (b-a)\gcd(b, a+b)$. From the fact that $a + 2b = \pm 1$ it follows $\gcd(a, b) = 1$ and so $\gcd(b, a + b) = 1$. Hence $h = (b-a)^2/(b-a) = b-a$ and because $b \equiv a \pmod{b-a}$, the condition (1) holds.

Corollary 1. *Let K be a cyclic algebraic number field of degree 3 over $\mathbb{Q}$. Let the matrix $\mathbf{A} = \mathrm{circ}_3(a, b, b)$ satisfy assumptions of Theorem 1 and transform a normal basis of the order B to a normal basis $(\gamma_1, \gamma_2, \gamma_3)$ of the order C, where $C \subseteq B$. Then any polynomial cycle of $f \in \mathbb{Z}[X]$ contains at most one of the elements $\gamma_1, \gamma_2, \gamma_3$.*

Proof. From [3, Theorem 1] it follows that if a number γ_i ($i = \{1, 2, 3\}$) does not generate the power basis of order C, then two of elements $\gamma_1, \gamma_2, \gamma_3$ cannot be in the same polynomial cycle for a polynomial with rational integral coefficients. So it is sufficient to prove that γ_i (for example γ_1) does not generate a power basis of C.

Let $(\beta_1, \beta_2, \beta_3)$ be a normal basis of an order B. Let matrix $\mathbf{A} = \mathrm{circ}_3(a, b, b)$ satisfy the assumption of Theorem 1. Then the matrix $\mathbf{A}$ transforms the basis $(\beta_1, \beta_2, \beta_3)$ to the basis $(\gamma_1, \gamma_2, \gamma_3)$, where

$$(\gamma_1, \gamma_2, \gamma_3) = (\beta_1, \beta_2, \beta_3)\mathbf{A}^{\mathrm{T}}\,.$$

Because the basis $(\beta_1, \beta_2, \beta_3)$ is a normal basis of an order, thus

$$\beta_1 + \beta_2 + \beta_3 = \pm 1$$

holds, and

$$\gamma_1 = a\beta_1 + b(\beta_2 + \beta_3) = a\beta_1 + b(\pm 1 - \beta_1) = (a-b)\beta_1 \pm b\,.$$

Elements γ_2 and γ_3 can be composed similarly, and we obtain the basis $(\gamma_1, \gamma_2, \gamma_3)$ in the form

$$\begin{aligned}\gamma_1 &= (a-b)\beta_1 \pm b\,,\\ \gamma_2 &= (a-b)\beta_2 \pm b\,,\\ \gamma_3 &= (a-b)\beta_3 \pm b\,.\end{aligned}$$

We consider the basis $(1, \gamma_1, \gamma_1^2)$, where

$$\gamma_1^2 = (a-b)^2\beta_1^2 \pm 2b(a-b)\beta_1 + b^2$$

the basis $(\beta_1, \beta_2, \beta_3)$ is an integral basis, therefore there exist $b_1, b_2, b_3 \in \mathbb{Z}$ such that

$$\begin{aligned}\gamma_1^2 &= (a-b)^2(b_1\beta_1 + b_2\beta_2 + b_3\beta_3) \pm 2b(a-b)\beta_1 + b^2\\ &= \big((a-b)b_1 \pm 2b\big)(a-b)\beta_1 + (a-b)^2 b_2\beta_2 + (a-b)^2 b_3\beta_3 + b^2\,.\end{aligned}$$

Let

$$\begin{aligned}s_1 &= (a-b)b_1 \pm 2b\,,\\ s_2 &= (a-b)b_2\,,\\ s_3 &= (a-b)b_3\,.\end{aligned}$$

Then

$$\begin{aligned}&\gamma_1^2 = s_1(a-b)\beta_1 + s_2(a-b)\beta_2 + s_3(a-b)\beta_3 + b^2\\ &= s_1\big((a-b)\beta_1 \pm b\big) + s_2\big((a-b)\beta_2 \pm b\big) + s_3\big((a-b)\beta_3 \pm b\big) + b^2 \mp (s_1+s_2+s_3)b\\ &= s_1\gamma_1 + s_2\gamma_2 + s_3\gamma_3 + b^2 \mp (s_1+s_2+s_3)b\end{aligned}$$

Because $\gamma_1 + \gamma_2 + \gamma_3 = \pm 1$, we can write

$$b^2 \mp (s_1+s_2+s_3)b = r(\gamma_1+\gamma_2+\gamma_3)\,,$$

so

$$\gamma_1^2 = (s_1+r)\gamma_1 + (s_2+r)\gamma_2 + (s_3+r)\gamma_3\,.$$

Suppose that $(\gamma_1, \gamma_2, \gamma_3)$ and $(1, \gamma_1, \gamma_1^2)$ are bases of the order C over $\mathbb{Z}$. Then the matrix $\mathbf{C}$ transforming the basis $(\gamma_1, \gamma_2, \gamma_3)$ to the basis $(1, \gamma_1, \gamma_1^2)$ has determinant equals ± 1. But

$$\det \mathbf{C} = \pm \begin{vmatrix} 1 & 1 & s_1+r\\ 1 & 0 & s_2+r\\ 1 & 0 & s_3+r\end{vmatrix} = \pm(s_2 - s_3) = \pm(a-b)(b_2-b_3)$$

where $a, b, b_2, b_3 \in \mathbb{Z}$, which is a contradiction to $a \equiv b \pmod{h}$, where $h \neq \pm 1$.

References

[1] Borevich, Z. I. and 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., On cycles of polynomials with integral rational coefficients, *Mathematica Slovaca*, to appear.

[4] Kostra, J., Orders with a normal basis, *Czechoslovak Math. Journal* **35** 110, 1985.

Z. Divišová
Department of Mathematics
University of Ostrava
30. dubna 22
Ostrava, Czech Republic
E-mail: zuzana.divisova@osu.cz

J. Kostra
Department of Mathematics
University of Ostrava
30. dubna 22
Ostrava, Czech Republic
E-mail: juraj.kostra@osu.cz

M. Pomp
Department of Mathematics
University of Ostrava
30. dubna 22
Ostrava, Czech Republic
E-mail: marek.pomp@osu.cz