BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(76), 2014, Pages 38–48
ISSN 1024–7696

Equivalence of pairs of matrices with relatively prime determinants over quadratic rings of principal ideals

Natalija Ladzoryshyn, Vasyl' Petrychkovych

Abstract. A special equivalence of matrices and their pairs over quadratic rings is investigated. It is established that for the pair of $n \times n$ matrices A, B over the quadratic rings of principal ideals $\mathbb{Z}[\sqrt{k}]$, where $(detA, detB) = 1$, there exist invertible matrices $U \in GL(n, \mathbb{Z})$ and $V^A, V^B \in GL(n, \mathbb{Z}[\sqrt{k}])$ such that $UAV^A = T^A$ and $UBV^B = T^B$ are the lower triangular matrices with invariant factors on the main diagonals.

Mathematics subject classification: 15A21, 11R04.
Keywords and phrases: Quadratic ring, matrices over quadratic rings, equivalence of pairs of matrices.

1 Introduction

Many problems in the representation theory of finite-dimensional algebras, in matrix factorizations over polynomial and other rings, etc. require to study some types of equivalences of matrices and their finite collections over various domains and to construct their canonical forms with respect to these equivalences [1–7]. These equivalences of matrices are such that their appropriate transformation matrices belong to certain subgroups of the general linear group.

In the analytical number theory concerning the study of arithmetic functions, in particular, the Kloosterman sum and its generalizations in matrix rings [8, 9], in the group theory [10], in the graph theory [11–13], etc. in [14, 15] it is necessary to investigate the structure of matrices over quadratic rings, in particular, over the ring of Gaussian integers.

In this paper we investigate the equivalence of matrices and their pairs: $A \to UAV^A$, $(A, B) \to (UAV^A, UBV^B)$ over quadratic rings $\mathbb{Z}[\sqrt{k}]$, where $U \in GL(n, \mathbb{Z})$, $V^A, V^B \in GL(n, \mathbb{Z}[\sqrt{k}])$. It is established that a pair of matrices A, B with relatively prime determinants over the quadratic principal ideal ring can be reduced by means of such equivalent transformations to the pair T^A, T^B of triangular forms with invariant factors on the main diagonals. Note that in [16] such a form was established with respect to this equivalence for matrices over the Euclidean quadratic rings.

2 Preliminaries

Let $\mathbb{Z}$ be a ring of integers. Then $\mathbb{K} = \mathbb{Z}[\sqrt{k}]$ is a quadratic ring, where $k \neq 0, 1$ is a square-free element of $\mathbb{Z}$. Elements $a \in \mathbb{Z}[\sqrt{k}]$ and their algebraic norm $N(a) \in \mathbb{Z}$ are determined in the following way [17]:

– if $k \equiv 2, 3 \pmod 4$, then

$$\mathbb{Z}[\sqrt{k}] = \{x + y\sqrt{k} \mid \; x, y \in \mathbb{Z}\}, \quad N(x + y\sqrt{k}) = x^2 - ky^2;$$

– if $k \equiv 1 \pmod 4$, then

$$\mathbb{Z}[\sqrt{k}] = \left\{ \frac{x}{2} + \frac{y}{2}\sqrt{k} \;\middle|\; x, y \in \mathbb{Z}, x - y \text{ divided by } 2 \right\}, \; N\left(\frac{x}{2} + \frac{y}{2}\sqrt{k}\right) = \frac{1}{4}(x^2 - ky^2).$$

If $\mathbb{K}$ is a Euclidean quadratic ring, then the Euclidean norm $E(a) \in \mathbb{N}$ of an element $a \in \mathbb{K}$ can be expressed as:

$$E(a) = \begin{cases} N(a) & \text{if } \mathbb{K} \text{ is imaginary,} \\ \\ |N(a)| & \text{if } \mathbb{K} \text{ is a real Euclidean quadratic ring.} \end{cases} \tag{1}$$

The quadratic ring $\mathbb{K} = \mathbb{Z}[\sqrt{k}]$ is called real if $k > 0$. If $k < 0$, then it is called an imaginary quadratic ring. Note that the algebraic and Euclidean norms of elements of the quadratic ring are completely multiplicative, i. e. $N(ab) = N(a)N(b)$, $E(ab) = E(a)E(b)$ for any $a, b \in \mathbb{K}$.

It is known that among quadratic rings there is a finite number of Euclidean quadratic rings [18, 19], among them there are quadratic principal ideal rings which are non-Euclidean, for example, the rings $\mathbb{Z}[\sqrt{k}]$, for $k = -19, -43, -67, -163$. There are some quadratic rings that are not principal ideal rings, for example, the ring $\mathbb{Z}[\sqrt{-5}]$.

In what follows $\mathbb{K}$ will denote a quadratic principal ideal ring, $U(\mathbb{K})$ a group of units of $\mathbb{K}$ and $\mathbb{K}_a$ will denote a complete set of residues modulo $a \in \mathbb{K}$.

Lemma 1. *Let $a_1, a_2, a_3 \in \mathbb{K}$ and let $d = (a_1, a_2, a_3)$ be their greatest common divisor. Then there exist elements $x_1, x_2 \in \mathbb{Z}$, $(x_1, x_2) = 1$, such that*

$$(x_1 a_1 + x_2 a_2, \, a_3) = d. \tag{2}$$

Proof. Obviously, it is sufficient to prove the lemma for the case where d equals 1. Write a_3 as a product of primes of $\mathbb{K}$, namely, $a_3 = ubc$, where $u \in U(\mathbb{K})$, $b = \prod_{i=1}^{l} p_i^{r_i}$, $p_i \neq \bar{p}_j$, $i \neq j$, $i, j = 1, \dots, l$, i.e. among p_i there are no pairwise conjugate elements, $c = \prod_{i=1}^{f} q_i^{s_i} \bar{q}_i^{t_i}$, i.e. all the divisors of c are pairwise conjugate elements.

Putting $d = 1$ in (2) yields

$$(x_1 a_1 + x_2 a_2, \, b) = 1 \quad \text{and} \quad (x_1 a_1 + x_2 a_2, \, c) = 1.$$

Since $(a_1, a_2, b) = 1$, then both a_1 and a_2 are not divisible by p_i, $i = 1, \dots, l$. Let

$$\mathrm{P}_1 = \prod_{i=1}^{l_1} p_i, \quad \mathrm{P}_2 = \prod_{i=l_1+1}^{l_2} p_i, \quad \mathrm{P}_3 = \prod_{i=l_2+1}^{l} p_i,$$

where $p_i \mid a_1$, (p_i divides a_1), $i = 1, \dots, l_1$, $p_i \mid a_2$, $i = l_1+1, \dots, l_2$, $p_i \nmid a_1a_2$, (p_i does not divide a_1a_2), $i = l_2+1, \dots, l$.

If $(x_1, x_2) = 1$ and

$$x_2 \not\equiv 0 \pmod{N(p_i)}, \quad i = 1, \dots, l_1, \tag{3}$$

the equality $(x_1a_1 + x_2a_2,\, \mathrm{P}_1) = 1$ holds.

Let us assume that some elements $\bar{p}_{l_1+1}, \dots, \bar{p}_{l_{21}}$, $l_{21} \le l_2$ divide a_1 and $\bar{p}_{l_{21}+1}, \dots, \bar{p}_{l_2}$ do not divide a_1, where $\bar{p}_i$, $i = l_1+1, \dots, l_2$, are conjugate elements to the corresponding primes p_i of the product P_2.

If

$$x_1 \not\equiv 0 \pmod{N(p_i)}, \; i = l_1+1, \dots, l_2, \tag{4}$$

$$\begin{cases} x_2 \not\equiv 0 \pmod{N(p_i)} \text{ if } i = l_1+1, \dots, l_{21}, \\ x_2 \equiv 0 \pmod{N(p_i)} \text{ if } i = l_{21}+1, \dots, l_2, \end{cases} \tag{5}$$

then $(x_1a_1 + x_2a_2,\, \mathrm{P}_2) = 1$.

Suppose that some prime elements $\bar{p}_{l_2+1}, \dots, \bar{p}_{l_{31}}$, $l_{31} \le l$, divide a_1 and $\bar{p}_{l_{31}+1}, \dots, \bar{p}_l$ do not divide a_1, where $\bar{p}_i$, $i = l_2+1, \dots, l$, are conjugate elements to the corresponding prime divisors p_i of the product P_3.

If

$$\begin{cases} x_2 \not\equiv 0 \pmod{N(p_i)}, \quad x_1 \equiv 0 \pmod{N(p_i)} \text{ if } i = l_2+1, \dots, l_{31}, \\ x_2 \equiv 0 \pmod{N(p_i)} \text{ if } i = l_{31}+1, \dots, l, \end{cases} \tag{6}$$

then $(x_1a_1 + x_2a_2,\, \mathrm{P}_3) = 1$.

Note that in the conditions (3)–(5) we considered that all prime divisors p_i, $i = 1, \dots, l_2$, of the products $\mathrm{P}_1, \mathrm{P}_2$ are not integers, i.e. $p_i \in \mathbb{K}$, but $p_i \notin \mathbb{Z}$. If some prime divisors p_i, $1 \le i \le l_2$, of the products $\mathrm{P}_1, \mathrm{P}_2$ are integers, i.e. $p_i \in \mathbb{Z}$, then in these conditions we consider the congruence (or incongruence) modulo p_i of these prime integer divisors.

Consequently, for the indicated $x_1, x_2 \in \mathbb{Z}$, we have $(x_1a_1 + x_2a_2,\, b) = 1$.

From $(a_1, a_2, c) = 1$ it follows that both a_1 and a_2 are not divisible by q_i and $\bar{q}_i$, $i = 1, \dots, f$. Write c as a product of primes of $\mathbb{K}$, i.e.

$$\mathrm{Q}_i = \prod_{j=f_{i-1}+1}^{f_i} q_j \quad \text{and} \quad \bar{\mathrm{Q}}_i = \prod_{j=f_{i-1}+1}^{f_i} \bar{q}_j, \quad i = 1, \dots, 6, \quad f_6 = f,$$

where we set $f_0 = 0$ and $(\mathrm{Q}_1\bar{\mathrm{Q}}_1\mathrm{Q}_2\bar{\mathrm{Q}}_3, a_1) = \mathrm{Q}_1\bar{\mathrm{Q}}_1\mathrm{Q}_2\bar{\mathrm{Q}}_3$, $(\bar{\mathrm{Q}}_2\bar{\mathrm{Q}}_4\mathrm{Q}_5\bar{\mathrm{Q}}_5, a_2) = \bar{\mathrm{Q}}_2\bar{\mathrm{Q}}_4\mathrm{Q}_5\bar{\mathrm{Q}}_5$, $(\mathrm{Q}_6\bar{\mathrm{Q}}_6, a_1a_2) = 1$.

Then

i) $(x_1a_1 + x_2a_2,\ \mathrm{Q}_1\bar{\mathrm{Q}}_1\mathrm{Q}_2\bar{\mathrm{Q}}_2\mathrm{Q}_3\bar{\mathrm{Q}}_3) = 1$ if

$$x_2 \not\equiv 0 \pmod{N(\mathrm{Q}_1\mathrm{Q}_2\mathrm{Q}_3)}, \tag{7}$$

$$\begin{cases} x_1 \not\equiv 0 \pmod{N(\mathrm{Q}_2)}, \\ x_1 \equiv 0 \pmod{N(\mathrm{Q}_3)}; \end{cases} \tag{8}$$

ii) $(x_1a_1 + x_2a_2,\ \mathrm{Q}_4\bar{\mathrm{Q}}_4\mathrm{Q}_5\bar{\mathrm{Q}}_5\mathrm{Q}_6\bar{\mathrm{Q}}_6) = 1$ if

$$x_2 \equiv 0 \pmod{N(\mathrm{Q}_4\mathrm{Q}_5\mathrm{Q}_6)}. \tag{9}$$

Consequently, under the imposed conditions, $(x_1a_1+x_2a_2,\ c) = 1$ holds and completes the proof. □

3 Equivalence of matrices

Let $M(m,n,\mathbb{K})$ and $M(n,\mathbb{K})$ be the sets of $m \times n$ and $n \times n$ matrices over the quadratic principal ideal ring $\mathbb{K}$, respectively; d_k^A be the greatest common divisor of minors of order k of the matrix A and $A^{(m,n)}$ be an $m \times n$ matrix.

It is known that an $n \times n$ matrix A over the commutative principal ideal domain R is equivalent to the canonical diagonal form (the Smith normal form) [20], i.e. there exist invertible matrices $U, V \in GL(n,R)$ such that

$$D^A = UAV = diag(\mu_1^A, \dots, \mu_r^A, 0, \dots, 0),$$

$\mu_i^A | \mu_{i+1}^A$, $i = 1, \dots, r-1$, μ_i^A are called invariant factors of matrix A.

Lemma 2. *Let $A \in M(m,n,\mathbb{K})$, $m \le n$, $rangA = m$. Then there exists a row $\mathbf{x} = \|x_1 \ \dots \ x_m\|$, $x_1, \dots, x_m \in \mathbb{Z}$, such that*

$$\mathbf{x}A = \|a'_{11} \ \dots \ a'_{1n}\|,$$

where $(a'_{11}, \dots, a'_{1n}) = d_1^A$.

Proof. We proceed by induction on m. Without loss of generality, we may assume that $d_1^A = 1$.

Let $m = 2$, i.e.

$$A^{(2,n)} = \left\| \begin{matrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \end{matrix} \right\|.$$

It is known [20] that there exists a matrix $V \in GL(n,\mathbb{K})$ such that

$$A^{(2,n)}V = \left\| \begin{matrix} a_1 & 0 & 0 & \dots & 0 \\ a_2 & a_3 & 0 & \dots & 0 \end{matrix} \right\|.$$

Since $\left\| \, x_1 \quad x_2 \, \right\| A^{(2,n)}V = \left\| \, x_1a_1 + x_2a_2 \quad x_2a_3 \quad 0 \quad \dots \quad 0 \, \right\|$, then we prove that there exist $x_1, x_2 \in \mathbb{Z}$ such that $(x_1a_1 + x_2a_2,\, x_2a_3) = 1$.

By Lemma 1 there exist $x_1, x_2 \in \mathbb{Z}$, $(x_1, x_2) = 1$, such that $(x_1a_1 + x_2a_2,\, a_3) = 1$. If $(x_2, a_1) = 1$ and x_1, x_2 satisfy the conditions (3)–(9), then $(x_1a_1 + x_2a_2,\, x_2a_3) = 1$.

Note that if the only prime divisors of a_3 and their conjugates $p_i, \bar{p}_i$, $q_j, \bar{q}_j$, $i = 1, \dots, l$, $j = 1, \dots, f$, are the divisors of a_1 then, under the imposed conditions, the equality $(x_2, a_1) = 1$ holds.

Let us assume that $g_1, \dots, g_s$, among g_i, $i = 1, \dots, s$, there are non-conjugate elements and $h_1, \bar{h}_1, \dots, h_t, \bar{h}_t$ are the prime divisors of a_1, moreover $g_i, \bar{g}_i, h_j, \bar{h}_j$, $i = 1, \dots, s$, $j = 1, \dots, t$ do not divide a_3.

If

$$x_2 \not\equiv 0 \pmod{N(h_j)}, \quad j = 1, \dots, t, \tag{10}$$

$$x_2 \not\equiv 0 \pmod{N(g_i)} \quad \text{if} \quad g_i \in \mathbb{K},\ g_i \notin \mathbb{Z}, \quad i = 1, \dots, s, \tag{11}$$

then $(x_2, a_1) = 1$.

If some primes $g_1, \dots, g_v \in \mathbb{Z}$, $v \leq s$ and if

$$x_2 \not\equiv 0 \pmod{g_i}, \quad i = 1, \dots, v, \tag{12}$$

then the equality $(x_2, a_1) = 1$ holds. Consequently, under the imposed integers $x_1, x_2 \in \mathbb{Z}$ the equality $(x_1a_1 + x_2a_2,\, x_2a_3) = 1$ holds. It is obvious that $d_1^{A^{(2,n)}} = (a_1, a_2, a_3)$, and hence lemma is true for $m = 2$.

Let us assume that the lemma is true for $m - 1$, i.e. for the matrix

$$A^{(m-1,n)} = \begin{Vmatrix} a_{21} & \dots & a_{2n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{Vmatrix}$$

there exists a row $\left\| x'_2 \quad \dots \quad x'_m \right\|$, $x'_i \in \mathbb{Z}$, $i = 2, \dots, m$, such that

$$\left\| x'_2 \quad \dots \quad x'_m \right\| A^{(m-1,n)} = \left\| a'_{21} \quad \dots \quad a'_{2n} \right\|,$$

where $(a'_{21}, \dots, a'_{2n}) = d_1^{A^{(m-1,n)}}$ and $a'_{2j} = \sum\limits_{i=2}^{m} x'_i a_{ij}$, $j = 1, \dots, n$.

Let us prove the lemma for any arbitrary m. Consider the matrix

$$A_1^{(2,n)} = \begin{Vmatrix} a_{11} & \dots & a_{1n} \\ a'_{21} & \dots & a'_{2n} \end{Vmatrix}.$$

By the induction hypothesis the lemma is true for $m = 2$, i. e. there exists the row $\left\| x \quad y \right\|$, $x, y \in \mathbb{Z}$, such that

$$\left\| x \quad y \right\| A_1^{(2,n)} = \left\| a'_{11} \quad \dots \quad a'_{1n} \right\|,$$

where $(a'_{11},\dots,a'_{1n}) = d_1^{A_1^{(2,n)}}$, $a'_{1j} = xa_{11} + y\sum\limits_{i=2}^{m} x'_i a_{ij}$, $j = 1,\dots,n$. Since $d_1^{A_1^{(2,n)}} = d_1^A$, then there exists the row $\mathbf{x} = \left\|x_1 \ \ \dots \ \ x_m\right\|$, where $x_1 = x$, $x_i = yx'_i$, $i = 2,\dots,m$, such that

$$\mathbf{x}A = \left\|a'_{11} \ \ \dots \ \ a'_{1n}\right\|$$

and $(a'_{11},\dots,a'_{1n}) = d_1^A$. Hence, the lemma is proved for any m, and the induction is completed. □

Theorem 1. *Let $A \in M(n,\mathbb{K})$, $detA \neq 0$. Then there exist invertible matrices $U \in GL(n,\mathbb{Z})$ and $V \in GL(n,\mathbb{K})$ such that*

$$UAV = \left\|\begin{matrix} \mu_1^A & 0 & \dots & 0 \\ t_{21}^A\mu_1^A & \mu_2^A & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1}^A\mu_1^A & t_{n2}^A\mu_2^A & \dots & \mu_n^A \end{matrix}\right\| = T^A, \tag{13}$$

where $t_{ij}^A \in \mathbb{K}_{\delta_{ij}^A}$, $\delta_{ij}^A = \frac{\mu_i^A}{\mu_j^A}$, $i,j = 1,\dots,n$, $i > j$.

Proof. Let $A = \left\|a_{ij}\right\|_1^n$, $a_{ij} \in \mathbb{K}$, $i,j = 1,\dots,n$. By Lemma 2 there exists a row $\mathbf{x} = \left\|x_1 \ \ \dots \ \ x_n\right\|$, $x_1,\dots,x_n \in \mathbb{Z}$, such that

$$\mathbf{x}A = \left\|a'_{11} \ \ \dots \ \ a'_{1n}\right\|,$$

where $(a'_{11},\dots,a'_{1n}) = d_1^A$. There exists an invertible matrix $U = \left\|\begin{matrix} x_1 & \dots & x_n \\ & * & \end{matrix}\right\|$ such that

$$UA = \left\|\begin{matrix} a'_{11} & \dots & a'_{1n} \\ & * & \end{matrix}\right\| = A_1,$$

where $(a'_{11},\dots,a'_{1n}) = d_1^A$ and $*$ are some elements. Then for some matrix $V_1 \in GL(n,\mathbb{K})$ we obtain:

$$A_1V_1 = UAV_1 = \left\|\begin{array}{c|c} \mu_1^A & \mathbf{0} \\ \hline \tilde{a}_{21}\mu_1^A & \\ \vdots & A^{(n-1,n-1)} \\ \tilde{a}_{n1}\mu_1^A & \end{array}\right\|,$$

where $\mu_1^A = d_1^{A_1} = d_1^A$ and μ_1^A divides all the elements of matrix $A^{(n-1,n-1)}$. Hence, μ_1^A is the first invariant factor of A.

Applying the similar reasoning to matrix $A^{(n-1,n-1)}$, after a finite number of steps we reduce matrix A by these transformations to the following triangular form with invariant factors on the main diagonal:

$$\tilde{A} = \left\|\begin{matrix} \mu_1^A & 0 & \dots & 0 \\ \tilde{a}_{21}\mu_1^A & \mu_2^A & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{a}_{n1}\mu_1^A & \tilde{a}_{n2}\mu_2^A & \dots & \mu_n^A \end{matrix}\right\|.$$

Let $\mathbb{K}_{\delta_{21}^A}$ be a prescribed complete set of residues modulo $\delta_{21}^A = \frac{\mu_2^A}{\mu_1^A}$. Since $\mu_2^A = \mu_1^A \delta_{21}^A$, then $\tilde{a}_{21} \equiv t_{21}^A \pmod{\delta_{21}^A}$, where $t_{21}^A \in \mathbb{K}_{\delta_{21}^A}$. Then $\tilde{a}_{21} = t_{21}^A + q\delta_{21}^A$, where $q \in \mathbb{K}$. Let us construct the invertible matrix $W_1 = \begin{Vmatrix} 1 & 0 \\ -q & 1 \end{Vmatrix} \oplus I^{(n-2)}$, where $I^{(n-2)}$ is an identity matrix of order $n-2$. Thus, we get matrix $\tilde{A}W_1$ whose $(2,1)$ element is equal to $t_{21}^A \mu_1^A$. Now we carry out a similar reasoning for non-diagonal elements of the third and the last rows of matrix $\tilde{A}$, and reduce this matrix to matrix T^A of the form (13). Therefore, the proof of the theorem is completed. $\square$

4 Equivalence of pairs of matrices

Lemma 3. *Let $A, B \in M(m,n,\mathbb{K})$, $m \le n$ and $(d_m^A, d_m^B) = 1$. Then there exists a row $\mathbf{x} = \|x_1 \quad \dots \quad x_m\|$, $x_1, \dots, x_m \in \mathbb{Z}$, such that*

$$\mathbf{x}A = \|a'_{11} \quad \dots \quad a'_{1n}\|, \quad \mathbf{x}B = \|b'_{11} \quad \dots \quad b'_{1n}\|,$$

where $(a'_{11}, \dots, a'_{1n}) = d_1^A$, $(b'_{11}, \dots, b'_{1n}) = d_1^B$.

Proof. Let $A = \|a_{ij}\|_1^{m,n}$, $B = \|b_{ij}\|_1^{m,n}$, $a_{ij}, b_{ij} \in \mathbb{K}$, $i = 1, \dots, m$, $j = 1, \dots, n$. Without loss of generality, we may assume that $d_1^A = d_1^B = 1$. Let us prove the lemma for $m = 2$. Consider the matrices

$$A^{(2,n)} = \begin{Vmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \end{Vmatrix}, \quad B^{(2,n)} = \begin{Vmatrix} b_{11} & \dots & b_{1n} \\ b_{21} & \dots & b_{2n} \end{Vmatrix}.$$

By Theorem 1 for the matrix $B^{(2,n)}$ there exist matrices $U \in GL(2,\mathbb{Z})$ and $V_1 \in GL(n,\mathbb{K})$ such that

$$UB^{(2,n)}V_1 = \begin{Vmatrix} 1 & 0 & 0 & \dots & 0 \\ b_1 & b_2 & 0 & \dots & 0 \end{Vmatrix} = B_1.$$

Then for the matrix $UA^{(2,n)}$ there exists a matrix $V_2 \in GL(n,\mathbb{K})$ such that

$$UA^{(2,n)}V_2 = \begin{Vmatrix} a_1 & 0 & 0 & \dots & 0 \\ a_2 & a_3 & 0 & \dots & 0 \end{Vmatrix} = A_1.$$

We need to prove that for the pair of matrices A_1, B_1 there exists a row $\|x_1 \quad x_2\|$, $x_1, x_2 \in \mathbb{Z}$, such that

$$\| \; x_1 \quad x_2 \; \| A_1 = \| \; x_1a_1 + x_2a_2 \quad x_2a_3 \quad 0 \quad \dots \quad 0 \; \|,$$

$$\| \; x_1 \quad x_2 \; \| B_1 = \| \; x_1 + x_2b_1 \quad x_2b_2 \quad 0 \quad \dots \quad 0 \; \|,$$

where

$$(x_1a_1 + x_2a_2,\, x_2a_3) = 1, \tag{14}$$

$$(x_1 + x_2 b_1,\, x_2 b_2) = 1. \tag{15}$$

By Lemma 1 and by Lemma 2, the equality (14) holds if x_1, x_2 satisfy the conditions (3)–(12).

Now we choose such $x_1, x_2 \in \mathbb{Z}$, $(x_1, x_2) = 1$, that both (14) and (15) hold.

It is sufficient to prove (14), (15) for the case of $\bar{p}_1, \dots, \bar{p}_{l_{11}}$, $1 \le l_{11} \le l_1$; $\bar{p}_{l_{21}+1}, \dots, \bar{p}_{l_{22}}$, $l_{21} + 1 \le l_{22} \le l_2$; $\bar{p}_{l_{31}+1}, \dots, \bar{p}_{l_{32}}$, $l_{31} + 1 \le l_{32} \le l$; $\bar{g}_1, \dots, \bar{g}_{s_1}$, $1 \le s_1 \le s$, are prime divisors of b_2, where $\bar{p}_i$ and $\bar{g}_j$ are conjugate primes to the corresponding prime divisors p_i, g_j of the elements a_3 and a_1 of matrix A_1.

If

$$\begin{cases} x_1 \equiv 0 \pmod{N(p_i)} & \text{if } \bar{p}_i \nmid b_1, \\ x_1 \not\equiv 0 \pmod{N(p_i)} & \text{if } \bar{p}_i \mid b_1,\ i = 1, \dots, l_{11}, \end{cases}$$

then $(x_1 + x_2 b_1,\, \bar{p}_1 \dots \bar{p}_{l_{11}}) = 1$.

The equalities $(x_1 + x_2 b_1,\, \bar{p}_{l_{21}+1} \dots \bar{p}_{l_{22}}) = 1$ and $(x_1 + x_2 b_1,\, \bar{p}_{l_{31}+1} \dots \bar{p}_{l_{32}}) = 1$ hold, in case x_1, x_2 satisfy the conditions (4)–(6).

Now if

$$\begin{cases} x_1 \equiv 0 \pmod{N(g_i)} & \text{if } \bar{g}_i \nmid b_1, \\ x_1 \not\equiv 0 \pmod{N(g_i)} & \text{if } \bar{g}_i \mid b_1, \quad i = 1, \dots, s_1, \end{cases}$$

then $(x_1 + x_2 b_1,\, \bar{g}_1 \dots \bar{g}_{s_1}) = 1$.

Hence, there exists a row $\mathbf{x} = \left\| x_1 \quad x_2 \right\|$, where $x_1, x_2 \in \mathbb{Z}$, such that for the rows $\mathbf{x}A_1$ and $\mathbf{x}B_1$ the equalities (14), (15) are true. Then in Lemma 3 the mentioned row for matrices $A^{(2,n)}, B^{(2,n)}$ is the row $\tilde{\mathbf{x}} = \left\| x_1 \quad x_2 \right\| U$. The lemma is true for $m = 2$. Furthermore, we prove the lemma by induction, similarly as in the proof of Lemma 2. This completes the proof. $\square$

Theorem 2. *Let $A, B \in M(n, \mathbb{K})$ and $(det A, det B) = 1$. Then there exist invertible matrices $U \in GL(n, \mathbb{Z})$ and $V^A, V^B \in GL(n, \mathbb{K})$ such that*

$$UAV^A = \begin{Vmatrix} \mu_1^A & 0 & \dots & 0 \\ t_{21}^A \mu_1^A & \mu_2^A & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1}^A \mu_1^A & t_{n2}^A \mu_2^A & \dots & \mu_n^A \end{Vmatrix} = T^A, \tag{16}$$

$$UBV^B = \begin{Vmatrix} \mu_1^B & 0 & \dots & 0 \\ t_{21}^B \mu_1^B & \mu_2^B & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1}^B \mu_1^B & t_{n2}^B \mu_2^B & \dots & \mu_n^B \end{Vmatrix} = T^B, \tag{17}$$

where $t_{ij}^A \in \mathbb{K}_{\delta_{ij}^A}$, $\delta_{ij}^A = \frac{\mu_i^A}{\mu_j^A}$, $\quad t_{ij}^B \in \mathbb{K}_{\delta_{ij}^B}$, $\delta_{ij}^B = \frac{\mu_i^B}{\mu_j^B}$; $\quad i, j = 1, \dots, n,\ i > j$.

Proof. Let $A = \|a_{ij}\|_1^n$, $B = \|b_{ij}\|_1^n$, $a_{ij},\ b_{ij} \in \mathbb{K}$, $i,j = 1,\dots,n$. By Lemma 3 there exists a row $\mathbf{x} = \|x_1 \ \ \dots \ \ x_n\|$, $x_1,\dots,x_n \in \mathbb{Z}$, such that

$$\mathbf{x}A = \|a'_{11} \ \ \dots \ \ a'_{1n}\|, \qquad \mathbf{x}B = \|b'_{11} \ \ \dots \ \ b'_{1n}\|,$$

where $(a'_{11},\dots,a'_{1n}) = d_1^A$ and $(b'_{11},\dots,b'_{1n}) = d_1^B$. There is an invertible matrix $U \in GL(n,\mathbb{Z})$ with the first row $\|x_1 \ \ \dots \ \ x_n\|$. Thus,

$$UA = \begin{Vmatrix} a'_{11} & \dots & a'_{1n} \\ & * & \end{Vmatrix} = A_1 \qquad \text{and} \qquad UB = \begin{Vmatrix} b'_{11} & \dots & b'_{1n} \\ & * & \end{Vmatrix} = B_1.$$

Then there exist matrices $V_1, V_2 \in GL(n,K)$ such that

$$A_1V_1 = \left\Vert \begin{array}{c|c} \mu_1^A & \mathbf{0} \\ \hline \tilde{a}_{21}\mu_1^A & \\ \vdots & A^{(n-1,n-1)} \\ \tilde{a}_{n1}\mu_1^A & \end{array} \right\Vert, \qquad B_1V_2 = \left\Vert \begin{array}{c|c} \mu_1^B & \mathbf{0} \\ \hline \tilde{b}_{21}\mu_1^B & \\ \vdots & B^{(n-1,n-1)} \\ \tilde{b}_{n1}\mu_1^B & \end{array} \right\Vert,$$

where $\mu_1^A = d_1^A$, $\mu_1^B = d_1^B$.

We carry out a similar reasoning for matrices $A^{(n-1,n-1)}$ and $B^{(n-1,n-1)}$, after a finite number of steps we reduce matrices A and B by the indicated transformations to the triangular forms

$$\tilde{A} = \begin{Vmatrix} \mu_1^A & 0 & \dots & 0 \\ \tilde{a}_{21}\mu_1^A & \mu_2^A & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{a}_{n1}\mu_1^A & \tilde{a}_{n2}\mu_2^A & \dots & \mu_n^A \end{Vmatrix}, \qquad \tilde{B} = \begin{Vmatrix} \mu_1^B & 0 & \dots & 0 \\ \tilde{b}_{21}\mu_1^B & \mu_2^B & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{b}_{n1}\mu_1^B & \tilde{b}_{n2}\mu_2^B & \dots & \mu_n^B \end{Vmatrix}.$$

Thus, we will reduce the pair of matrices $\tilde{A}, \tilde{B}$ to the pair T^A, T^B of the form (16), (17) by means of the indicated transformations in the same way as we reduced matrix $\tilde{A}$ to matrix T^A at the end of Theorem 1. This completes the proof of the theorem. □

Remark. Note that the pair of matrices $A, B \in M(n,\mathbb{K})$ such that $(detA, detB) = d \neq 1$ cannot be reduced by means of the indicated transformations to the pair of matrices T^A, T^B of the form (16), (17).

Example. Let

$$A = \begin{Vmatrix} 1+\sqrt{-2} & 0 \\ 0 & 1-\sqrt{-2} \end{Vmatrix}, \qquad B = \begin{Vmatrix} 1 & 0 \\ 3+\sqrt{-2} & (1+\sqrt{-2})(1-\sqrt{-2}) \end{Vmatrix}$$

be 2×2 matrices over the Euclidean quadratic ring $\mathbb{Z}[\sqrt{-2}]$. It is easy to verify that the pair of matrices A, B, $(detA, detB) = 1$ cannot be reduced by these transformations to pairs T^A, T^B of the form (16), (17).

Corollary. *Let* $\mathbb{K}$ *be a Euclidean quadratic ring,* $A, B \in M(n, \mathbb{K})$, $(detA, detB) = 1$, $E(a)$ *be the Euclidean norm of element* $a \in \mathbb{K}$, *determined by (1). Then there exist invertible matrices* $U \in GL(n, \mathbb{Z})$ *and* $V^A, V^B \in GL(n, \mathbb{K})$ *such that*

$$UAV^A = \begin{Vmatrix} \mu_1^A & 0 & \dots & 0 \\ t_{21}^A \mu_1^A & \mu_2^A & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1}^A \mu_1^A & t_{n2}^A \mu_2^A & \dots & \mu_n^A \end{Vmatrix}, \qquad UBV^B = \begin{Vmatrix} \mu_1^B & 0 & \dots & 0 \\ t_{21}^B \mu_1^B & \mu_2^B & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1}^B \mu_1^B & t_{n2}^B \mu_2^B & \dots & \mu_n^B \end{Vmatrix},$$

where

$$\begin{cases} t_{ij}^A = 0 \quad \textit{if} \quad \mu_i^A = \mu_j^A, \\ \\ E(t_{ij}^A) < E\left(\frac{\mu_i^A}{\mu_j^A}\right) \quad \textit{if} \quad \mu_i^A \neq \mu_j^A \ \textit{and} \ t_{ij}^A \neq 0, \ i, j = 1, \dots, n, \ i > j; \end{cases}$$

$$\begin{cases} t_{ij}^B = 0 \quad \textit{if} \quad \mu_i^B = \mu_j^B, \\ \\ E(t_{ij}^B) < E\left(\frac{\mu_i^B}{\mu_j^B}\right) \quad \textit{if} \quad \mu_i^B \neq \mu_j^B \ \textit{and} \ t_{ij}^B \neq 0, \ i, j = 1, \dots, n, \ i > j. \end{cases}$$

References

[1] Dlab V., Ringel C. M. *Canonical forms of pairs of complex matrices.* Linear Algebra Appl., 1991, **147**, 387–410.

[2] Gaiduk T. N., Sergeichuk V. V. *Generic canonical form of pairs of matrices with zeros.* Linear Algebra Appl., 2004, **380**, 241—251.

[3] Petrichkovich V. M. *Semiscalar equivalence and the Smith normal form of polynomial matrices.* J. Sov. Math., 1993, **66**, No. 1, 2030–2033.

[4] Dias da Silva J. A., Laffey T. J. *On simultaneous similarity of matrices and related questions.* Linear Algebra Appl., 1999, **291**, 167–184.

[5] Petrichkovich V. M. *Semiscalar equivalence and factorization of polynomial matrices.* Ukrainian Math. J., 1990, **42**, No. , 570–574.

[6] Kazimirs'kii P. S. *Decomposition of matrix polynomials into factors.* Naukova Dumka, Kiev, 1981 (in Ukrainian).

[7] Petrychkovych V. *Generalized equivalence of pairs of matrices.* Linear and Multilinear Algebra, 2000, **48**, No. 2, 179–188.

[8] Varbanets S. P. *General Kloosterman sums over ring of Gaussian integers.* Ukrainian Math. J., 2007, **59**, No. 9, 1313–1341.

[9] Velichko I. N. *Generalized Kloosterman sum over the matrix ring* $M_n(\mathbb{Z}[i])$. Visn. Odes. Nats. Univ., Ser. Mat. and Mekh., 2010, **15**, No. 19, 9–20 (in Russian).

[10] Nica B. *The unreasonable slightness of* E_2 *over imaginary quadratic rings.* Amer. Math. Monthly, 2011, **118**, No. 5, 455–462.

[11] Taylor G. *Cyclotomic matrices and graphs over the ring of integers of some imaginary quadratic fields.* J. Algebra, 2011, **331**, No. 1, 523–545.

[12] Taylor G. *Lehmer's conjecture for matrices over the ring of integers of some imaginary quadratic fields.* J. Number Theory, 2012, **132**, No. 4, 590–607.

[13] Greaves G. *Cyclotomic matrices over the Eisenstein and Gaussian integers.* J. Algebra, 2012, **372**, 560–583.

[14] Sidorov S. V. *On similarity of* 2×2 *matrices over the ring of Gaussian integers with reducible characteristic polynomial.* Vestn. Nizhni Novgorod Univ., 2008, **4**, 122–126 (in Russian).

[15] Rodosskii K. A. *The Euclidean algorithm.* Nauka, Moscow, 1988 (in Russian).

[16] Zelisko V. R., Ladzoryshyn N. B., Petrychkovych V. M. *On equivalence of matrices over quadratic Euclidean rings.* Appl. Problems of Mechanics and Math., 2006, **4**, 16–21 (in Ukrainian).

[17] Hasse H. *Number theory.* Classics in Mathematics, Springer-Verlag, New York-Berlin, 1980.

[18] Clark David A. *A quadratic field which is Euclidean but not norm-Euclidean.* Manuscripta Math., 1994, **83**, No. 3–4, 327–330.

[19] Harper Malcolm. $\mathbb{Z}[\sqrt{14}]$ *is Euclidean.* Canad. J. Math., 2004, **56**, No. 1, 55–70.

[20] Newman Morris. *Integral matrices.* Pure and Applied Mathematics, vol. 45, Academic Press, New York, 1972.

Natalija Ladzoryshyn, Vasyl' Petrychkovych
Pidstryhach Institute for Applied Problems of Mechanics
and Mathematics of the NAS of Ukraine
3b Naukova Str., 79060, L'viv
Ukraine

E-mail: *natalja.ladzoryshyn@gmail.com;*
vas_petrych@yahoo.com

Received May 30, 2014