Bull. Korean Math. Soc. **53** (2016), No. 6, pp. 1697–1705
http://dx.doi.org/10.4134/BKMS.b150889
pISSN: 1015-8634 / eISSN: 2234-3016

LINEAR ISOMORPHISMS OF NON-DEGENERATE INTEGRAL TERNARY CUBIC FORMS

Inhwan Lee and Byeong-Kweon Oh

Abstract. In this article, we consider the problem on finding non-degenerate n-ary m-ic forms having an $n\times n$ matrix A as a linear isomorphism. We show that it is equivalent to solve a linear diophantine equation. In particular, we find all integral ternary cubic forms having A as a linear isomorphism, for any $A \in GL_3(\mathbb{Z})$. We also give a family of non-degenerate cubic forms F such that $F(\mathbf{x}) = N$ always has infinitely many integer solutions if exists.

1. Introduction

A non-zero homogeneous polynomial

$$\begin{aligned} F(\mathbf{x}) &= F(x_1, x_2, \dots, x_n) \\ &= \sum_{\substack{e_1+\cdots+e_n=m \\ e_i \ge 0}} a_{e_1,\dots,e_n} x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}, \quad (a_{e_1,\dots,e_n} \in \mathbb{C}) \end{aligned}$$

is called an *n-ary m-ic form.* If $n = 2, 3$ or 4, then F is called a binary, ternary or quaternary form, respectively, and if $m = 2, 3$ or 4, then F is called a quadratic, cubic or quartic form, respectively. An n-ary m-ic form F is called *degenerate* if there is a k-ary ($k < n$) m-ic form G and a matrix $S = (s_{ij}) \in M_{kn}(\mathbb{C})$ such that

$$F(\mathbf{x}) = G(S\mathbf{x}) = G(s_{11}x_1 + \cdots + s_{1n}x_n, \dots, s_{k1}x_1 + \cdots + s_{kn}x_n).$$

Hence any degenerate form is singular, that is, the projective variety $F = 0$ on the projective space $\mathbb{P}^{n-1}$ is singular. Note that a quadratic form is non-singular if and only if it is non-degenerate.

An $n \times n$ matrix $A = (a_{ij})$ satisfying

$$F(A\mathbf{x}) := F(a_{11}x_1 + \cdots + a_{1n}x_n, \dots, a_{n1}x_1 + \cdots + a_{nn}x_n) = F(\mathbf{x})$$

Received October 29, 2015; Revised March 2, 2016.
2010 *Mathematics Subject Classification.* Primary 11E76, 15A63, 11D25.
Key words and phrases. linear isomorphisms, n-ary m-ic forms.
This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (No. 2011-0016437).

is called a *linear isomorphism* of F, and the group of all linear isomorphisms of F is denoted by $\mathrm{Lin}(F)$. Deciding this group for given non-degenerate n-ary m-ic form seems to be quite difficult problem even for quadratic form case. In 1880, Jordan proved in [4] that $\mathrm{Lin}(F)$ is finite if F is non-singular and $m \geq 3$ (see also [6], [8] and [9]).

Let F be an integral form, that is, $a_{e_1,\ldots,e_n} \in \mathbb{Z}$. We define

$$\mathrm{Lin}_{\mathbb{Z}}(F) := \mathrm{Lin}(F) \cap M_n(\mathbb{Z}),$$

which is called the *integral linear isomorphism group of* F. If F is an integral quadratic form, it is well known that $\mathrm{Lin}_{\mathbb{Z}}(F)$ is finite if and only if F is definite. For the structures of integral linear isomorphism groups of some quadratic forms, see [10] for an indefinite case, and [5] for a definite case.

There is little known on this group for $m \geq 3$. In fact, finding an integral linear isomorphism is equivalent to solve a system of diophantine equations. Related with computing integral linear isomorphism group, one may naturally ask, for an $A \in M_n(\mathbb{Z})$, whether or not an n-ary m-ic form F exists such that $A \in \mathrm{Lin}_{\mathbb{Z}}(F)$. The answer of this question is completely known on the quadratic form case. In Theorem 1 of [3], Horn and Merino classified all possible types of Jordan canonical forms of the complex orthogonal matrix. What they proved is that a matrix A whose Jordan canonical form is one of five types given in the theorem is an automorphism of a non-singular quadratic form defined over the complex numbers. However one may easily deduce that there also exists a non-singular integral quadratic form satisfying the above property if A is an integral matrix.

For $m, n \geq 3$, solving the diophantine equation $F(\mathbf{x}) = N$, for an integral form F and an integer N, is one of challenging problems in number theory. For example, as one of the simplest cases, it is not known whether or not the diophantine equation $x^3+y^3+z^3 = 33$ has an integer solution (see, for example, [2]).

If F is degenerate, then for any integer N, the equation $F(\mathbf{x}) = N$ always has infinitely many integer solutions if exists. If $\mathbf{x}_0$ is an integral solution of $F(\mathbf{x}) = N$ for some integer N, then $A\mathbf{x}_0$ is also an integer solution for any $A \in \mathrm{Lin}_{\mathbb{Z}}(F)$. According to these two observations, it seems to be interesting problem to find a non-degenerate form having an integral linear isomorphism whose order is infinite.

In this article, we consider the problem on finding non-degenerate forms having A as a linear isomorphism, for any $n \times n$ matrix A. We show that this is equivalent to solve a linear diophantine equation. In particular, we find all integral ternary cubic forms having A as a linear isomorphism, for any invertible matrix $A \in M_3(\mathbb{Z})$. We also give a family of non-degenerate cubic forms F such that $F(\mathbf{x}) = N$ always has infinitely many integer solutions if exists.

2. Linear isomorphisms of n-ary m-ic forms

For positive integers m and n, we define

$$\mathfrak{D}_m^n := \{(d_1, d_2, \ldots, d_n) \in \mathbb{Z}^n : \sum_{i=1}^{n} d_i = m,\ d_i \geq 0\}.$$

For two $\mathbf{d} = (d_1, d_2, \ldots, d_n),\ \mathbf{e} = (e_1, e_2, \ldots, e_n) \in \mathfrak{D}_m^n$, we define a lexicographic order $>$ by

$$\mathbf{d} > \mathbf{e} \quad \Longleftrightarrow \quad \text{there is an } i \text{ such that } d_k = e_k \text{ for any } k < i \text{ and } d_i > e_i.$$

For n indeterminates $x_1, x_2, \ldots, x_n$ and $\mathbf{e} = (e_1, e_2, \ldots, e_n) \in \mathfrak{D}_m^n$, we define a monomial $\mathbf{x}^{\mathbf{e}} = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ of degree m. Note that there is a one-to-one correspondence between the set of all monomials of degree m with n indeterminates and the set $\mathfrak{D}_m^n$. For an indeterminate vector $\mathbf{x} = (x_1, x_2, \ldots, x_n)^t$, we define an operator

$$\mathfrak{U}_m^n(\mathbf{x}) := (\mathbf{x}^{\mathbf{e}_1}, \mathbf{x}^{\mathbf{e}_2}, \ldots, \mathbf{x}^{\mathbf{e}_{H(n,m)}})^t,$$

where $\mathbf{e}_1 > \mathbf{e}_2 > \cdots > \mathbf{e}_{H(n,m)}$ are all elements in $\mathfrak{D}_m^n$ and $H(n, m)$ is the combination with repetition.

For a matrix $A \in M_n(\mathbb{C})$, assume that $(y_1, y_2, \ldots, y_n)^t = A(x_1, x_2, \ldots, x_n)^t$. Then for any $\mathbf{e} = (e_1, e_2, \ldots, e_n) \in \mathfrak{D}_m^n$, there are $a_{\mathbf{e},\mathbf{d}} \in \mathbb{C}$ such that

$$\mathbf{y}^{\mathbf{e}} = y_1^{e_1} y_2^{e_2} \cdots y_n^{e_n} = \sum_{\mathbf{d} \in \mathfrak{D}_m^n} a_{\mathbf{e},\mathbf{d}} \mathbf{x}^{\mathbf{d}}.$$

Now we define $\mathfrak{U}_m^n(A) := (a_{\mathbf{e}_i,\mathbf{e}_j}) \in M_{H(n,m)}(\mathbb{C})$, where $\mathbf{e}_i$ is the i-th element in $\mathfrak{D}_m^n$ in the lexicographic order. Note that $\mathfrak{U}_m^n(\mathbf{y}) = \mathfrak{U}_m^n(A)\mathfrak{U}_m^n(\mathbf{x})$.

Lemma 2.1. *The map $\mathfrak{U}_m^n : GL_n(\mathbb{C}) \to GL_{H(n,m)}(\mathbb{C})$ is a multiplicative homomorphism. In particular, if a matrix $A \in M_n(\mathbb{C})$ is similar to B, then $\mathfrak{U}_m^n(A)$ is also similar to $\mathfrak{U}_m^n(B)$ for any positive integer m.*

Proof. For any $A, B \in GL_n(\mathbb{C})$ and an indeterminate vector

$$\mathbf{x} = (x_1, x_2, \ldots, x_n)^t,$$

note that

$$\mathfrak{U}_m^n(AB)\mathfrak{U}_m^n(\mathbf{x}) = \mathfrak{U}_m^n(AB\mathbf{x}) = \mathfrak{U}_m^n(A)\mathfrak{U}_m^n(B\mathbf{x}) = \mathfrak{U}_m^n(A)\mathfrak{U}_m^n(B)\mathfrak{U}_m^n(\mathbf{x}).$$

It is well known the set $\{\mathfrak{U}_m^n(\mathbf{x}) : \mathbf{x} \in \mathbb{C}^n\}$ spans the vector space $\mathbb{C}^{H(n,m)}$. Therefore $\mathfrak{U}_m^n(AB) = \mathfrak{U}_m^n(A)\mathfrak{U}_m^n(B)$. □

Lemma 2.2. *For any $A \in M_n(\mathbb{C})$, $\det(\mathfrak{U}_m^n(A)) = \det(A)^{H(m,n)}$.*

Proof. Note that the matrix A is similar to an upper-triangular matrix, that is, there is a $T \in GL_n(\mathbb{C})$ such that $A = T^{-1}UT$, where $U = (u_{ij})$ is an upper-triangular matrix. For this upper-triangular matrix U, one may easily show that $\mathfrak{U}_m^n(U)$ is also upper-triangular and

$$\mathfrak{U}_m^n(U)_{\mathbf{e},\mathbf{e}} = u_{11}^{e_1} u_{22}^{e_2} \cdots u_{nn}^{e_n},$$

where $\mathbf{e} = (e_1, e_2, \ldots, e_n)$. Therefore

$$\det(\mathfrak{U}^n_m(A)) = \det(\mathfrak{U}^n_m(U)) = \det(U)^f,$$

where $H(n, m) \cdot m = nf$. Note that $f = \frac{m}{n} H(n, m) = H(m, n)$. The lemma follows from this. □

For positive integers m and n, let

$$F_m(\mathbf{x}) = F_m(x_1, x_2, \ldots, x_n) = \sum_{\mathbf{e} \in \mathfrak{D}^n_m} a_{\mathbf{e}} \mathbf{x}^{\mathbf{e}} \qquad (a_{\mathbf{e}} \in \mathbb{C}) \tag{2.1}$$

be an n-ary m-ic form. Recall that $\mathrm{Lin}(F_m)$ denotes the group of all linear isomorphisms of F_m. If a matrix A is similar to B with the transition matrix S, that is, $B = S^{-1}AS$, then one may easily show that

$$A \in \mathrm{Lin}(F_m) \iff B \in \mathrm{Lin}(F_m \circ S). \tag{2.2}$$

For the form F_m in (2.1), we define $\mathfrak{U}^n_m(F_m) := (a_{\mathbf{e}_1}, a_{\mathbf{e}_2}, \ldots, a_{\mathbf{e}_{H(n,m)}})^t \in \mathbb{C}^{H(n,m)}$.

Theorem 2.3. *Let F_m be a form given in* (2.1)*. Then $A \in Lin(F_m)$ if and only if $\mathfrak{U}^n_m(F_m)$ is the eigenvector of $\mathfrak{U}^n_m(A)^t$ corresponding to the eigenvalue* 1.

Proof. Note that $F_m(\mathbf{x}) = \mathfrak{U}^n_m(F_m)^t \cdot \mathfrak{U}^n_m(\mathbf{x})$. Hence

$$\begin{aligned} F_m(A\mathbf{x}) = F_m(\mathbf{x}) \quad &\iff \mathfrak{U}^n_m(F_m)^t \cdot \mathfrak{U}^n_m(A\mathbf{x}) = \mathfrak{U}^n_m(F_m)^t \cdot \mathfrak{U}^n_m(\mathbf{x}) \\ &\iff \mathfrak{U}^n_m(F_m)^t \mathfrak{U}^n_m(A) \mathfrak{U}^n_m(\mathbf{x}) = \mathfrak{U}^n_m(F_m)^t \cdot \mathfrak{U}^n_m(\mathbf{x}). \end{aligned}$$

Therefore $\mathfrak{U}^n_m(A)^t \cdot \mathfrak{U}^n_m(F_m) = \mathfrak{U}^n_m(F_m)$. The theorem follows from this. □

Let A be an $n \times n$ complex matrix and $f_A(x)$ be its characteristic polynomial. We define

$$\mathfrak{U}^n_m(f_A)(x) := \prod_{\mathbf{e} \in \mathfrak{D}^n_m} (x - \mathbf{\Lambda}^{\mathbf{e}}),$$

where $\mathbf{\Lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_n)$ and $\lambda_1, \lambda_2, \ldots, \lambda_n$ are all eigenvalues of A counting multiplicities. For the $\mathbb{C}$-vector space of n-ary m-ic forms

$$\mathfrak{S}_m(A) = \{F_m \mid F_m(A\mathbf{x}) = F_m(\mathbf{x})\},$$

the dimension of $\mathfrak{S}_m(A)$ is denoted by $d_m(A)$.

Theorem 2.4. *Under the assumptions given above, we have*

(i) *the characteristic polynomial of $\mathfrak{U}^n_m(A)$ is $\mathfrak{U}^n_m(f_A)(x)$;*
(ii) *there is an n-ary m-ic form F_m having A as a linear isomorphism if and only if $\mathfrak{U}^n_m(f_A)(1) = 0$;*
(iii) *if A is diagonalizable, then $d_m(A)$ is the algebraic multiplicity of the eigenvalue one of $\mathfrak{U}^n_m(A)$;*
(iv) *if n divides m and $\det(A)^{\frac{m}{n}} = 1$, then there is an n-ary m-ic form having A as a linear isomorphism, and*
(v) *if A is an integral matrix, then there is a basis for $\mathfrak{S}_m(A)$ consisting of integral forms.*

Proof. Choose a matrix T such that $TAT^{-1} = U = (u_{ij})$ is upper-triangular and $u_{ii} = \lambda_i$ $(1 \le i \le n)$. For any $\mathbf{e} \in \mathfrak{D}_m^n$, note that $\mathfrak{U}_m^n(U)_{\mathbf{e},\mathbf{f}} = 0$ for any $\mathbf{f} < \mathbf{e}$ and $\mathfrak{U}_m^n(U)_{\mathbf{e},\mathbf{e}} = \mathbf{\Lambda}^{\mathbf{e}}$. This implies that $\mathfrak{U}_m^n(U)$ is also upper-triangular and all of its eigenvalues are of the form $\mathbf{\Lambda}^{\mathbf{e}}$ for any $\mathbf{e} \in \mathfrak{D}_m^n$. Hence (i), (ii) and (iii) follow directly from Theorem 2.3. For (iv), note that $\mathfrak{U}_m^n(U)$ has an eigenvalue 1. Finally, assume that A is an integral matrix. Since

$$\mathfrak{S}_m(A) = \{\mathbf{x} \in \mathbb{C}^{H(n,m)} : \mathfrak{U}_m^n(A)^t(\mathbf{x}) = \mathbf{x}\}$$

and $\mathfrak{U}_m^n(A)$ is also integral, there are integral vectors that spans $\mathfrak{S}_m(A)$. □

Assume that $A \in SL_n(\mathbb{Z})$ and the characteristic polynomial $f_A(x)$ of A is a non-cyclotomic and irreducible polynomial. It is well known that A is a linear isomorphism of a non-degenerate integral quadratic form if and only if f_A is reciprocal, that is, $f_A(x) = x^n f_A(\frac{1}{x})$ (see [3]). For a cubic case, we only have the following partial result.

Proposition 2.5. *Under the assumptions given above, if the splitting field of $f_A(x)$ is abelian and n is not divisible by 3, then there does not exist an n-ary cubic form having A as a linear isomorphism.*

Proof. Since $f_A(x)$ is not cyclotomic by assumption, any root of it is not a third root of unity. Suppose that $\alpha^2\beta = 1$ for some roots α and β of $f_A(x)$. Since the Galois group of the splitting field of $f_A(x)$ acts on the set of roots transitively, there is a root δ of $f_A(x)$ such that $\beta^2\delta = 1$. Hence $\delta = \alpha^4$ is also a root of $f_A(x)$. This implies that α is a root of unity, which is a contradiction. It was proved in [1] that any product of three roots of $f_A(x)$ is not one under the assumptions given above. Therefore we have $\mathfrak{U}_3^n(f_A)(1) \neq 0$. The proposition follows from Theorem 2.4(ii). □

3. Linear isomorphisms of ternary cubic forms

Let $F_m(\mathbf{x}) = F_m(x_1, x_2, \ldots, x_n)$ be an n-ary m-ic form as in (2.1). We call F_m is *reducible over* $\mathbb{C}$ if $F_m(\mathbf{x}) = F_k(\mathbf{x}) \cdot F_{m-k}(\mathbf{x})$, where F_k and F_{m-k} are forms of degree k and $m-k$, respectively. If F_m is a product of m linear forms, then F_m is said to be *completely reducible over* $\mathbb{C}$. If the above forms F_k and F_{m-k} have integral coefficients, then we say that the integral form F_m is reducible over $\mathbb{Z}$.

For an n-ary m-ic form F_m, the Hessian matrix $H(F_m)$ of F_m is the square matrix defined by

$$H(F_m) = \begin{bmatrix} \frac{\partial^2 F}{\partial x_1^2} & \frac{\partial^2 F}{\partial x_1 \partial x_2} & \cdots & \frac{\partial^2 F}{\partial x_1 \partial x_n} \\ \frac{\partial^2 F}{\partial x_2 \partial x_1} & \frac{\partial^2 F}{\partial x_2^2} & \cdots & \frac{\partial^2 F}{\partial x_2 \partial x_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial^2 F}{\partial x_n \partial x_1} & \frac{\partial^2 F}{\partial x_n \partial x_2} & \cdots & \frac{\partial^2 F}{\partial x_n^2} \end{bmatrix}.$$

The determinant of $H(F_m)$ is denoted by $h(F_m)$. In general, $h(F_m)$ is the n-ary $n(m-2)$-ic form for any $m, n \geq 3$. If $G(\mathbf{x}) = F_m(A\mathbf{x})$, then

$$H(G)(\mathbf{x}) = A^t \cdot H(F_m)(A\mathbf{x}) \cdot A \quad \text{and} \quad h(G)(\mathbf{x}) = \det(A)^2 h(F_m)(A\mathbf{x}).$$

Lemma 3.1. *Let A be a 3×3 integral matrix such that $\det(A) \neq \pm 1$. If an integral cubic form F satisfies $F(A\mathbf{x}) = F(\mathbf{x})$, then F is degenerate.*

Proof. Note that F is degenerate if and only if $h(F) = 0$ (see, for example, [7]). Suppose that there is a nonzero vector $\mathbf{x}_0$ such that $h(F)(\mathbf{x}_0) \neq 0$. For a prime p dividing $\det(A)$, take an integer k such that $p^{2k} \nmid h(F)(\mathbf{x}_0)$. Since $F(A^k\mathbf{x}) = F(\mathbf{x})$, $h(F)(\mathbf{x}_0) = \det(A)^{2k} h(F)(A^k\mathbf{x}_0)$. This is a contradiction. □

Let T be a matrix in $GL_3(\mathbb{Z})$. We apply our results obtained in the previous section to find all (non-degenerate) integral ternary cubic forms having the matrix T as a linear isomorphism. To find such form, we need to compute eigenvectors of $\mathfrak{U}_3^3(T)$ corresponding to the eigenvalue one. If we find a form having a matrix rationally similar to T as a linear isomorphism, we may easily find a form having T as a linear isomorphism by (2.2).

Let $f_T(x)(m_T(x))$ be the characteristic (minimal, respectively) polynomial of T. First we assume that $T \in SL_3(\mathbb{Z})$ and $f_T(x) = x^3 - sx^2 - tx - 1$ for some $s, t \in \mathbb{Z}$. Let α, β and γ be all roots of $f_T(x)$ counting multiplicities and let $\Delta_f = t^2s^2 - 4s^3 + 4t^3 - 18ts - 27$ be the discriminant of f_T. Suppose that f_T has a multiple root $\alpha \in \mathbb{C}$, that is, $\Delta_f = 0$. Then one may easily show that $\alpha = \pm 1$. Hence f_T is $(x-1)^3$ or $(x-1)(x+1)^2$, which implies that $(s,t) = (3,-3)$ or $(-1,1)$. Note that these are all integral solutions of the diophantine equation $\Delta_f = 0$.

Suppose that $\deg(m_T) = 3$. Since T is rationally equivalent to its companion matrix, we may assume that $T = \left[\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & t \\ 0 & 1 & s \end{smallmatrix}\right]$. Note that the characteristic polynomial of 10×10 matrix $\mathfrak{U}_3^3(T)$ is of the form

$$f_{\mathfrak{U}_3^3(T)}(x) = (x-1)g_{s,t}(x)h_{s,t}(x),$$

where $g_{s,t}(x)$ is the monic polynomial of degree 3 with roots $\alpha^3, \beta^3, \gamma^3$, and $h_{s,t}(x)$ is the monic polynomial of degree 6 with roots $\alpha^2\beta, \alpha^2\gamma, \ldots, \beta\gamma^2$. Note that $g_{s,t}(1) = 0$ if and only if $s = -t$, and $h_{s,t}(1) = 0$ if and only if $\Delta_f = 0$. The latter holds only when $(s,t) = (3,-3)$ or $(-1,1)$ as stated above.

Suppose that $s \neq -t$. Then T is diagonalizable and $d_3(T) = 1$. In this case, we can take

$$\begin{aligned} F_{s,t}(x,y,z) := {} & x^3 + sx^2y + (2t+s^2)x^2z - txy^2 - (ts+3)xyz \\ & + (t^2-2s)xz^2 + y^3 + sy^2z - tyz^2 + z^3. \end{aligned}$$

as a generator of $\mathfrak{S}_3(T)$. Note that $F_{s,t}$ is non-degenerate and completely reducible over $\mathbb{C}$.

Now assume that $s = -t$. Then $f_{\mathfrak{U}_3^3(T)}(x) = (x-1)^2u(x)v(x)w(x)$, where $u(x) = x^2+x+1+2sx-s^2x$, $v(x) = x^2-s^3x+3s^2x-2x+1$, $w(x) = x^2+x-sx+1$.

Hence, if $s=-t$ and $s\neq 0,-1,3$, then $d_3(T)\le 2$. In fact, $d_3(T)=2$ in this case, and one may take a basis for $\mathfrak{S}_3(T)$ consisting of

$$G_{1,s}(x,y,z):=(x+y+z)(x^2+y^2+z^2-xy-yz-(1+3s)xz),$$
$$G_{2,s}(x,y,z):=(x+y+z)(xy+yz+(1+s)xz).$$

Note that $aG_{1,s}+bG_{2,s}$ is non-degenerate for any $a,b\in\mathbb{Z}$ with $b\neq 3a$ and is reducible over $\mathbb{Z}$.

If $(s,t)=(0,0)$, then $f_{\mathfrak{U}_3^3(T)}(x)=(x-1)^4(x^2+x+1)^3$ and $d_3(T)=4$. We may take a basis for $\mathfrak{S}_3(T)$ consisting of

$$x^3+y^3+z^3,\ x^2y+xz^2+y^2z,\ x^2z+xy^2+yz^2,\ xyz.$$

If $(s,t)=(-1,1)$, then $f_{\mathfrak{U}_3^3(T)}(x)=(x-1)^4(x+1)^6$ and $d_3(T)=2$. Note that $G_{1,-1}(x,y,z)$ and $G_{2,-1}(x,y,z)$ form a basis for $\mathfrak{S}_3(T)$. In this case, $aG_{1,-1}+bG_{2,-1}$ is degenerate for any $a,b\in\mathbb{Z}$.

If $(s,t)=(3,-3)$, then $f_{\mathfrak{U}_3^3(T)}(x)=(x-1)^{10}$ and $d_3(T)=2$. Note that $G_{1,3}(x,y,z)$ and $G_{2,3}(x,y,z)$ form a basis for $\mathfrak{S}_3(T)$. In this case, $aG_{1,3}+bG_{2,3}$ is non-degenerate for any $a,b\in\mathbb{Z}$ with $b\neq 3a$.

Now suppose that $\deg(m_T)<3$. In this case, f_T must have a multiple root. Hence $(s,t)=(3,-3)$ or $(-1,1)$, i.e., $f_T(x)=(x-1)^3$ or $(x-1)(x+1)^2$.

If $f_T(x)=(x-1)^3$, then $m_T(x)=x-1$ or $(x-1)^2$. The former case implies that $T=I$, which is a linear isomorphism of any cubic form. Assume that $m_T(x)=(x-1)^2$. Since T is rationally similar to its Jordan canonical form, we may assume that $T=\begin{bmatrix}1&0&0\\0&1&1\\0&0&1\end{bmatrix}$. By a direct computation, we have $f_{\mathfrak{U}_3^3(T)}(x)=(x-1)^{10}$ and $d_3(T)=4$. Every cubic form in $\mathfrak{S}_3(T)$ is of the form

$$ax^3+bx^2z+cxz^2+dz^3,$$

which is degenerate for arbitrary integers a,b,c,d .

If $f_T(x)=(x-1)(x+1)^2$ and $m_T(x)=(x-1)(x+1)$, then we assume that $T=\mathrm{diag}(1,-1,-1)$. By a direct computation, we have $f_{\mathfrak{u}_3^3(T)}(x)=(x-1)^4(x+1)^6$ and $d_3(T)=4$. Furthermore every cubic form in $\mathfrak{S}_3(T)$ is of the form

$$ax^3+bxy^2+cxyz+dxz^2,$$

which is non-degenerate for any integers a,b,c,d with $4bd-c^2\neq 0$, and is reducible over $\mathbb{Z}$.

Now assume that $\det(T)=-1$ and $f_T(x)=x^3-sx^2-tx+1$. By using similar method in the above, one may easily show that the cases when there is a non-degenerate form having T as a linear isomorphism are $(s,t)=(-1,-1)$, or $(s,t)=(1,1)$ and $m_T(x)=(x+1)(x-1)$. In the former case, $d_3(T)=2$ and every cubic form in $\mathfrak{S}_3(T)$ is of the form

$$a(x-y+z)(x^2-y^2+z^2-xy+yz-2xz)+by(x-z)(x-y+z),$$

and in the latter case, $d_3(T)=6$ and every cubic form in $\mathfrak{S}_3(T)$ is of the form

$$ax^3+bx^2y+cxy^2+dxz^2+ey^3+fyz^2.$$

Summing up all, we have the following theorem.

Theorem 3.2. *Let $T \in GL_3(\mathbb{Z})$ and let $f_T(x) = x^3 - sx^2 - tx - \det(T)$ be the characteristic polynomial of T. If $\det(T) = 1$, then there is a non-degenerate integral ternary cubic form having T as a linear isomorphism except the cases when $(s,t) = (-1,1)$ and $m_T(x) = (x-1)(x+1)^2$, or $(s,t) = (3,-3)$ and $m_T(x) = (x-1)^2$. If $\det(T) = -1$, then there is a non-degenerate integral ternary cubic form having T as a linear isomorphism if and only if $(s,t) = (-1,-1)$, or $(s,t) = (1,1)$ and $m_T(x) = (x-1)(x+1)$.*

Corollary 3.3. *Let $T \in GL_3(\mathbb{Z})$ be a matrix having infinite order and let F be an integral ternary cubic form such that $F(T\mathbf{x}) = F(\mathbf{x})$. Define*

$$R(F) := \{N \in \mathbb{Z} \mid F(\mathbf{x}) = N \text{ has an integer solution } \mathbf{x}_0 \text{ such that } T\mathbf{x}_0 \neq \mathbf{x}_0\}.$$

Then for any integer $N \in R(F)$, the diophantine equation $F(\mathbf{x}) = N$ has infinitely many integer solutions. In particular, if $s \neq -t$, then $F_{s,t}(x,y,z) = N$ always has infinitely many integer solutions for any integer N if exists.

Proof. Let $f_T(x) = x^3 - sx^2 - tx - \det(T)$ be the characteristic polynomial of T. We may assume that F is non-degenerate. Since we are assuming that the order of T is infinite, we may further assume that $\det(T) = 1$ and $m_T(x) = f_T(x)$. Assume that $F(\mathbf{x}_0) = N$ for some integral vector $\mathbf{x}_0$ which is not an eigenvector of T corresponding to the eigenvalue one. Since $F(T^m\mathbf{x}_0) = N$ for any integer m, it is enough to show that $T^u(\mathbf{x}_0) \neq T^v(\mathbf{x}_0)$ for any $u \neq v$. Suppose that $T^k\mathbf{x}_0 = \mathbf{x}_0$ for some integer k. Then T has a root of unity not equal to one as an eigenvalue. Therefore, the only possible candidate of (s,t) is $(3,-3)$. However, in this case, one may easily show that $\mathbf{x}_0$ should be an eigenvector of T corresponding to the eigenvalue one by a direct computation. This is a contradiction. Finally, note that if $s \neq -t$, then the matrix T does not have an eigenvalue one. □

Remark 3.4. Under the same assumptions as above, the number of solutions for the diophantine equation $F(\mathbf{x}) = N$ is one of $0, 1$ or ∞, for any integer N.

Remark 3.5. In the above corollary, if $F(\mathbf{x}_0) = N$ for some eigenvector $\mathbf{x}_0$ of T corresponding to the eigenvalue one, then $F(\mathbf{x}) = N$ could have exactly one integer solution. For example, if

$$T = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & -4 \\ 0 & 1 & 4 \end{bmatrix} \quad \text{and} \quad G_{2,4}(x,y,z) = (x+y+z)(xy+yz+5zx),$$

then the equation $G_{2,4}(x,y,z) = 1$ has only one solution $(1,-3,1)$, which is an eigenvector of T corresponding to the eigenvalue one.

References

[1] M. Drmota and M. Skalba, *Relations between polynomial roots*, Acta Arith. **71** (1995), no. 1, 65–77.

[2] A. Elsenhans and J. Jahnel, *New sum of three cubes*, Math. Comp. **78** (2009), no. 266, 1227–1230.

[3] R. A. Horn and D. I. Merino, *The Jordan canonical forms of complex orthogonal and skew-symmetric matrices*, Linear Algebra Appl. **302/303** (1999), 411–421.

[4] C. Jordan, *Memore sur l'equivalence des formes*, J. Ec. Pol. **XLVIII** (1880), 112–150.

[5] M.-H. Kim and B.-K. Oh, *Generation of isometries of certain $\mathbb{Z}$-lattices by symmetries*, J. Number Theory **83** (2000), no. 1, 76–90.

[6] H. Matsumura and P. Monsky, *On the automorphisms of hypersurfaces*, J. Math. Kyoto Univ. **3** (1964), 347–361.

[7] P. J. Olver, *Classical Invariant Theory*, London Mathematical Society Student Texts, Vol. 44, 1999.

[8] J. E. Schneider, *Orthogonal groups of nonsingular forms of higher degree*, J. Algebra **27** (1973), 112–116.

[9] H. Suzuki, *Automorphism groups of multilinear maps*, Osaka J. Math. **20** (1983), no. 3, 659–673.

[10] E. B. Vinberg, *The groups of units of certain quadratic forms*, (Russian) Mat. Sb. (N.S.) **87(129)** (1972), 18–36.

Inhwan Lee
Department of Mathematical Sciences
Seoul National University
Seoul 151-747, Korea
E-mail address: lih0905@snu.ac.kr

Byeong-Kweon Oh
Department of Mathematical Sciences and Research Institute of Mathematics
Seoul National University
Seoul 151-747, Korea
E-mail address: bkoh@snu.ac.kr