ON THE MATRICES KEEPING INVARIANT THE QUADRATIC FORMS

Alina-PETRESCU-NIȚĂ [1], Carmina GEORGESCU[2]

În această lucrare, se studiază matricele care invariază o formă pătratică reală fixată şi se dă un criteriu ca acestea să formeze un grup; în §1 se dau câteva exemple. În §3 se studiază grupul matricelor care invariază forma "pitagoreică" $x^2+y^2-z^2$ *şi se dă un procedeu de obținere sistematică a soluțiilor ecuației diofantice* $x^2+y^2=z^2$.

In this work, one analyzes conditions that a real quadratic form is kept invariant by some matrices. In §1 some examples are given and in §3, one studies the group of matrice which keep invariant the "pitagoreic" form $x^2+y^2-z^2$ *and one indicates a procedure to get systematically the solutions of the diophantic equation* $x^2+y^2=z^2$.

Keywords: Quadratic form, invariant, group of matrices, a pitagoreic group.

1. Introduction

Quadratic forms are important geometrical algebraic objects, both for the study of various mathematical structures, but also for their applications to the study of quadrics in matrix calculus, differential geometry and tensor calculation.

A general theoretical presentation is found in [1] and more specific problemes are treated in [2], [3]. Using [4], the paper deals with the study of matrices which preserve a real given quadratic form.

In the second part of the paper the results are applied to the systematic listing of Pythagorean triples of numbers 2. On the connection between matrices and quadratic forms.

[1] Lecturer, Depart. of Mathematics, University POLITEHNICA of Bucharest, Romania, e-mail: nita_alina@yahoo.com
[2] Lecturer, INRIA Rhone Aples, Inovall'ee, 655 avenue de l'Europe, 38330, Montbonnot, France, e-mail: carmina.georgescu@inrialpes.fr

2. On the connection between matrices and quadratic forms

Fix a real quadratic form $q:\mathbf{R}^n \to \mathbf{R}$. By definition, a matrix $A \in M_n(\mathbf{R})$ *keeps invariant the quadratic form* q if the following condition holds:

$$\text{for any} \quad \underline{x} = (x_1, \ldots x_n), \quad q(\underline{x}) = q(A \cdot \underline{x}) \tag{1}$$

we will identify $\underline{x}$ and its transpose $\underline{x}^T$.

We will denote by $G(q)$ the set of all matrices from $M_n(\mathbf{R})$ which keep invariant q.

If $Q \in M_n(\mathbf{R})$ is the matrix associated to q for the canonical basis of the space $\mathbf{R}^n$, it is well known the Q is symmetric and moreover, $q(x) = \underline{x}^T \cdot Q \cdot \underline{x}$, for any $\underline{x} \in \mathbf{R}^n$.

Proposition 1. *The condition* (1) *is equivalent to*

$$A^T \cdot Q \cdot A = Q \tag{2}$$

Proof. We have $q(x) = \underline{x}^T \cdot Q \cdot \underline{x}$ and

$$q(A \cdot \underline{x}) = (A \cdot x)^T \cdot Q \cdot A \cdot \underline{x} = \underline{x}^T \cdot A^T \cdot Q \cdot A \cdot \underline{x} \ .$$

The relation (1) becomes $\underline{x}^T \cdot Q \cdot \underline{x} = \underline{x}^T \cdot (A^T \cdot Q \cdot A) \cdot \underline{x}$, for any $\underline{x} \in \mathbf{R}^n$, whence (2).

Proposition 2. *The set* $G(q)$ *is stable to products*.

Proof. Let $A, B \in G(q)$. We have to prove that $B \cdot A \in G(q)$. But for any $\underline{x}, \underline{y} \in \mathbf{R}^n$, $q(\underline{x}) = q(A \cdot \underline{x})$ and $q(\underline{y}) = q(B \cdot \underline{y})$. Take $\underline{y} = A \cdot \underline{x}$, hence $q(\underline{x}) = q(A \cdot \underline{x}) = q(\underline{y}) = q(B \cdot \underline{y}) = q(B \cdot A \cdot \underline{x})$, for any $\underline{x} \in \mathbf{R}^n$.
In other terms, $B.A \in G(q)$.

Corollary. $G(q) \bigcap GL(n, \mathbf{R})$ *is a group with respect to multiplication of matrices.*

Proof. Obviously, the unit matrix I_n belongs to $G(q)$. If $A \in G(q)$ is nonsingular, we will show that $A^{-1} \in G(q)$. Indeed, for any $\underline{x} \in \mathbf{R}^n$ fixed, take $\underline{y} = A^{-1} \cdot \underline{x}$. By (1), $q(\underline{y}) = q(A \cdot \underline{y})$, hence $q(A^{-1} \cdot \underline{x}) = q(A \cdot A^{-1} \cdot \underline{x}) = q(\underline{x})$, therefore $A^{-1} \in G(q)$.

NOTE. Suppose that $n = 2$ and $q(x_1, x_2) = x_1^2$. The matrix $A = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ verifies (2) hence belongs to $G(q)$, but A is singular.

Proposition 3. *If q is nondegenerated, then $G(q)$ is a group relative to multiplication.*

Proof. By definition, q has all the proper values of the matrix Q (associated to q in the canonical basis) are different from zero, hence $\det Q \neq 0$. It is enough to show that any matrix $A \in G(q)$ is nonsingular; indeed, from the relation (2), it follows that $\det Q = (\det Q)(\det A)^2$, whence $(\det A)^2 = 1$. Therefore, $\det A \neq 0$ and A is nonsingular. It remains to apply the corollary of the Proposition 2.

Examples. 1. Take $q(x_1, \ldots, x_n) = x_1^2 + \cdots + x_n^2$. In this case, $Q = \dot{I}_n$ and the condition (2) becomes: $A^T \cdot A = \dot{I}_n$. Thus, A is an orthogonal matrix of order n. In the case $n = 2$, one obtain the rotation matrices.

2. Consider the case $n = 2$ and $q(x_1, x_2) = x_1^2 - x_2^2$.

In this case, $Q = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and if $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

keeps invariant q, then from (2) one gets: $a^2 - b^2 = 1$, $c^2 - d^2 = 1$ and $ab - cd = 0$. Then $a^2 = b^2 + 1 \neq 0$ and $c^2 = d^2 + 1 \neq 0$. If $b \neq 0$, then $\frac{a}{d} = \frac{c}{b} = k$, hence $k^2 = \frac{a^2}{d^2} = \frac{c^2}{b^2} = \frac{a^2 - c^2}{d^2 - b^2} = 1$. Therefore, $k = 1$ or $k = -1$.

So, $A = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$ or $A = \begin{pmatrix} a & b \\ -b & -a \end{pmatrix}$, with $a^2 - b^2 = 1$.

If $b = 0$, then $a^2 = 1$, $d = 0$ and we refind the above matrices.

3. In the case $n = 4$ and $q(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 - x_4^2$, which is nondegenerated, then the set $G(q)$ has a structure of group (by proposition 3), which can be called the group of *Lorentz transformations* of the 4-dimensional space of Einstein-Minkowski.

Other results are in [2].

3. The matrices which keep invariant the quadratic form $q : \mathbf{R}^3 \to \mathbf{R}$, $q(x, y, z) = x^2 + y^2 - z^2$.

In this case, $Q = \operatorname{diag}(1,1,-1)$ and by the proposition 3,

$$G(q) = \{A \in M_3(\mathbf{R}) \mid A^t \cdot Q \cdot A = Q\}$$

is a group relatively to multiplication (since q is nondegenerated).

If $A \in G(q)$, then $(\det A)^2 = 1$; whence $\det A = \pm 1$ and particularly, A is nonsingular. If $A = \begin{pmatrix} a & b & c \\ x & y & z \\ u & v & w \end{pmatrix}$, then by (2), it follows the system:

$$\begin{aligned} &a^2 + x^2 - u^2 = 1, \quad b^2 + y^2 - v^2 = 1, \quad c^2 + z^2 - w^2 = 1 \\ &ab + xy - uv = 1, \quad bc + yz - vw = 0, \quad ca + zx + wu = 0 \end{aligned}.$$

Proposition 4. *For $q = x^2 + y^2 - z^2$, the set $\mathcal{P} = G(q) \bigcap M_3(\mathbf{Z})$ is a group relatively to multiplication.*

Proof. Obviously, if $A, B \in \mathcal{P}$, then $A \cdot B \in \mathcal{P}$, by the proposition 2. It remains to prove that any matrix $A \in \mathcal{P}$ has an inverse in $\mathcal{P}$. Indeed, since $\det A = \pm 1$, it follows that $A^{-1} = \frac{1}{\det A} A^* = \pm A^*$, hence A^{-1} has all elements in $\mathbf{Z}$ and thus, $A^{-1} \in \mathcal{P}$.

Definition. By obvious reason, the group $\mathcal{P}$ can be called the *pitagoreic group* (connected by the diophantic equation $x^2 + y^2 = z^2$).

Whenever a 3-uple (x, y, z) is a solution of the equation $x^2 + y^2 = z^2$, then $q(x, y, z) = 0$ and by (1), the 3-uple $A(x, y, z)$ is also a solution of the same equation, for any $A \in \mathcal{P}$.

Consider the matrices

$$Q = \operatorname{diag}(1,1,-1),\ R = \operatorname{diag}(-1,1,1) \text{ and } S = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then $Q^2 = R^2 = S^2 = I_3$, hence $Q^{-1} = Q$, $R^{-1} = R$, $S^{-1} = S$. Denote by $\mathcal{P}_1$ the subgroup of $\mathcal{P}$ generated by Q, R, S, hence

$$\mathcal{P}_1 \subset \{Q^p \cdot R^q \cdot S^r \mid p, q, r \in \{0,1,-1\}\}.$$

By explicit calculus, $\mathcal{P}_1$ consists of the following 16 matrices:

$$\begin{aligned} &m_1 = \operatorname{diag}(1,1,1) = I_3, \quad m_2 = \operatorname{diag}(1,1,-1) = Q \\ &m_3 = \operatorname{diag}(1,-1,1), \quad m_4 = \operatorname{diag}(1,-1,-1), \\ &m_5 = \operatorname{diag}(-1,1,1) = R, \quad m_6 = \operatorname{diag}(-1,1,-1), \\ &m_7 = \operatorname{diag}(-1,-1,1), \quad m_8 = \operatorname{diag}(-1,-1,-1), \end{aligned}$$

$$m_9 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = S, \quad m_{10} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

$$m_{11} = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad m_{12} = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

$$m_{13} = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad m_{14} = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

$$m_{15} = \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad m_{16} = \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Theorem 1. a) $\mathcal{P}_1$ *is formed by the matrices of the form* $\operatorname{diag}(a,b,c)$ *or* $\begin{pmatrix} 0 & a & 0 \\ b & 0 & 0 \\ 0 & 0 & c \end{pmatrix}$, *where* $a,b,c \in \{-1,1\}$.

b) $\mathbf{P}_1 \neq \mathbf{P}$.

Proof. a) Represents the synthesis of the above explicitation.

b) We have to indicate a matrix $T \in \mathcal{P} \setminus \mathcal{P}_1$.

Consider the algebraic identitites

$$q(x,y,z) = x^2 + y^2 - z^2 = (x+y+z)^2 - 2(x+z)(y+z) \tag{3}$$

$$q(x,y,z) = (x+y+z)^2 - 2(z-x)(z-y) \tag{4}$$

and the linear map $t : \mathbf{R}^3 \to \mathbf{R}^3$, $t(x,y,z) = (x_1,y_1,z_1)$, where x_1, y_1, z_1 are given by the relations.

$$x_1 + y_1 - z_1 = x + y + z, \quad z_1 - x_1 = x + z, \quad z_1 - y_1 = y + z, \tag{5}$$

whence

$$q(x,y,z) \overset{by(3)}{=} (x_1 + y_1 - z_1)^2 - 2(z_1 - x_1)\cdot(z_1 - y_1) \overset{by(4)}{=} q(x_1,y_1,z_1).$$

Thus, $q(t(x,y,z)) = q(x,y,z)$, for any x,y,z, therefore the matrix T associated to the linear map t (in the canonical basis of $\mathbf{R}^3$) belongs to $\mathcal{P}$. On the other hand,

solving the linear system, it follows that $x_1 = x + 2y + 2z$, $y_1 = 2x + y + 2z$, $z_1 = 2x + 2y + 3z$ hence $T = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}$.

Since $T \neq m_k$, for any $1 \leq k \leq 16$, it follows that $T \notin \mathcal{P}_1$.

The matrix T is invertible with the inverse

$$T^{-1} = \begin{pmatrix} 1 & 2 & -2 \\ 2 & 1 & -2 \\ -2 & -2 & 3 \end{pmatrix}$$

and moreover, $q(T \cdot \underline{x}) = q(\underline{x})$, for any triple $\underline{x} \in \mathbf{Z}^3$.

We also consider the matrices

$$V = T \cdot m_5 = \begin{pmatrix} -1 & 2 & 2 \\ -2 & 1 & -2 \\ -2 & 2 & 3 \end{pmatrix}$$

and

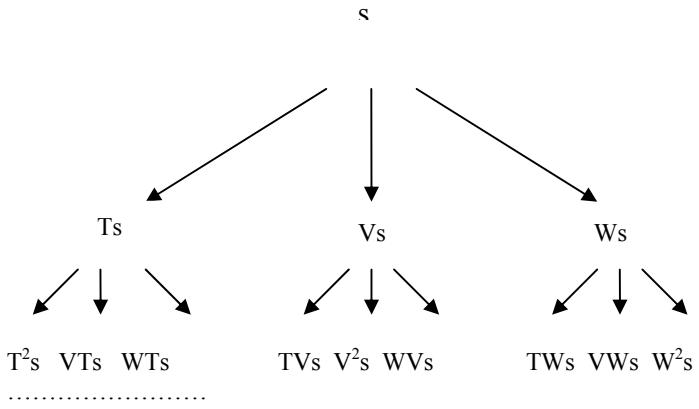
$$W = T \cdot m_3 = \begin{pmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{pmatrix}.$$

These matrices T, V, W belong to the group $G(q)$.

Definition. Two triples of pitagoreic numbers $u = (x, y, z)$, $v = (x', y', z')$, i.e. non-null solutions in $\mathbf{N}^3$ of the equation $x^2 + y^2 = z^2$ are said equivalent if there is $n \in \mathbf{N}^*$ such that either $v = n \cdot u$, or $u = n \cdot v$.

For instance, (1,0,1) and (3,4,5) are not equivalent, but (3,4,5) and (6,8,10) are equivalent.

Theorem 2. *Let* $s = (3,4,5)^T$ *be the standard solution of the equation* $x^2 + y^2 = z^2$ *in* $\mathbf{N}^3$. *The set* S *of all nonequivalent solutions in* $(\mathbf{N}^*)^3$ *of the equation* $x^2 + y^2 = z^2$ *is just the set of the vertices of the following ordered tree:*



In other terms, all the elements of S are obtained by starting with s and multiplying it with T,V,W taken in an arbitrary order.

Proof. If $(x,y,z)\in\mathcal{P}_1$, put $(p,q,r)^T = T^{-1}(x,y,z)^T$, that is

$$p = x+2y-2z,\ q = 2x+y-2z \text{ and } r = -2x-2y+3z.$$

One easily verifies that $0<r<z$ and p,q cannot be both negative. If $(x,y,z)\in S$ and $(x',y',z')^T = T\cdot(x,y,z)^T$, then $y'-x' = -(x-y)$ hence $|x-y|$ is preserved; then, $z'-x' = z+x$ and $z'-y' = z+y$, hence $z-x$ and $z-y$ increase. On the other hand, if $(x'',y'',z'')^T = V\cdot(x,y,z)^T$, then $y''-x'' = -(x+y)$ hence $|y-x|$ increases, $z''-x'' = z-x$ hence $z-x$ is preserved and $z''-y'' = z+y$, that is $z-y$ increases. Finally, if $(x''',y''',z''')^T = W\cdot(x,y,z)^T$, one gets $y'''-x''' = x+y$, $z'''-x''' = z+x$ and $z'''-y''' = z-y$, hence $y-x$, $z-x$ increase and $z-y$ is preserved.

Thus, startind from s, all the pitagoreic triples (a,b,c) such that $|a-b|=1$ are obtained by $T^n\cdot s$.

The pitagoreic triples (a,b,c) such that $c-b=1$ (or $c-a=1$) correspond to $V^n\cdot s$ and those having components that differ by 2, are obtained from $W^n\cdot s$.

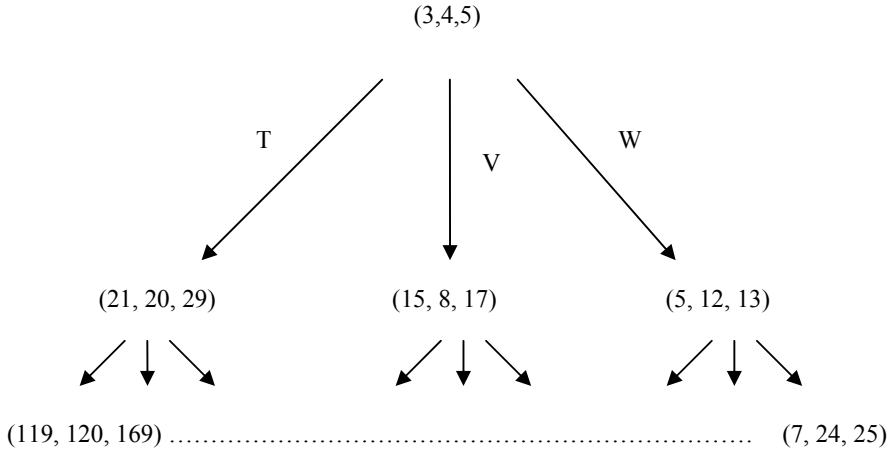
One can explicit the powers T^n,V^n,W^n (by diagonalisation of T,V,W). For instance, one gets that $V^n\cdot s = (4n^2+8n+3,\ 4n+4,\ 4n^2+8n+5)^T$ and

$W^n \cdot s = (2n+3,\ 2n^2+6n+4,\ 2n^2+6n+5)^T$, which correspond to the solutions of the form $(a,b,a+2)$ and respectively $(a,b,b+1)$ from the set S.

4. Conclusions

The main aim of the work is to study the group of all matrices which keep invariant the pitagoreic quadratic form $x^2+y^2-z^2$. One knows the classical parametrization of the set S of all triples of non-null natural numbers (x,y,z) such that $x^2+y^2=z^2$; namely $x=k\,|\,p^2-q^2\,|,\ \ y=2pqk,\ \ z=k(p^2+q^2)$, with $k,p,q\in\mathbf{N}^*,\ p\neq q$.

The theorem 2 allows another listing of the elements of S. At any level $\underline{r}$ of the above ordered tree, one get $3^{\underline{r}}$ solutions. Explicitly, starting with $s=(3,4,5)^T\equiv(3,4,5)$, are obtain



REFERENCES

[1] *Alina Niță*, Generalized inverse of a matrix with applications to optimization of some systems (PhD Thesis, in Romanian), Univ. of Bucharest, Faculty of Math. and Comp. Science, 2004
[2] *R. Godement ,* Cours d'algebre, Hermann, 1978
[3] *K. Kitacha,* Arithmetic of quadratic forms, Cambridge University Press, 1999
[4] *Z. Borevici, I.R. Safarevici,* Teoria numerelor, (Number theory), Ed.Stiintifica si Enciclopedica, 1985 (in Romanian)
[5] *D.Z. Djokovic, S. Severini*, Rational orthoganal versus real orthogonal, J. of Algebra, 18, 649-673, 2009.