THE FACTORIZATION OF AN INTEGRAL MATRIX INTO A PRODUCT OF TWO INTEGRAL SYMMETRIC MATRICES

BY OLGA TAUSKY

Communicated on January 31, 1973

A theorem going back to Frobenius, but refound repeatedly (for references see [5], generalized to arbitrary fields states:

Every $n \times n$ matrix $A = (a_{ik})$ with elements in a field $F$ is similar to its transpose $A'$:

(1) $A' = S^{-1}AS$

where $S$ can be chosen symmetric and with elements in $F$. This is equivalent to the fact that every $A$ can be expressed in the form

(2) $A = S_1S_2$

when $S_1, S_2$ are symmetric, with elements in $F$ where $S_1$ is nonsingular.

Here a new concept is introduced. It is a form of degree $n$ associated with the matrix.\(^2\) For relation (1) implies

(3) $SA' = AS$.

This leads to a set of linear equations for the elements of the symmetric matrix $S$. If $A$ has all its roots different (though the general case leads to relevant results too) then the number of $F$-independent symmetric solutions $S$ of (3) is $n$. The elements of $S$ are then linear forms in $n$ parameters and $\det S$ is a form of degree $n$ in $n$ variables. It is this form which plays an important role. If $A$ is replaced by a matrix similar to $A$ then $S$ undergoes a congruence transformation and the form is multiplied by a square factor in $F$.

For $n = 2$ relation (3) leads to a single equation in 3 variables. This equation is given by

(4) $a_{21}x_1 + (a_{22} - a_{11})x_2 - a_{12}x_3 = 0$

---

\(^1\) This work was carried out (in part) under an NSF contract; I have profited from discussions with E. Bender, J. Brillhart, E. C. Dade, D. Estes, H. Kisilevsky.

\(^2\) W. Givens informs me that he also considered such a form.
if $S = (z_1^t \ z_2^t)$. Apart from a multiple this form is given by

$$a(\lambda, \mu) = (\alpha_1\alpha_3 - \alpha_2^2)\lambda^2 + (\alpha_1\beta_3 - 2\alpha_2\beta_2 + \alpha_3\beta_1)\lambda\mu + (\beta_1\beta_3 - \beta_2^2)\mu^2$$

where $\alpha_1$, $\alpha_2$, $\alpha_3$ and $\beta_1$, $\beta_2$, $\beta_3$ are a pair of independent solutions of (4). It can be shown that the discriminant of (5) and the discriminant of the form

$$a_{21}x^2 + (a_{22} - a_{11})xy + a_{12}y^2$$

differ by a square factor. The latter discriminant is also the discriminant of the characteristic polynomial of $A$.

The emphasis of the present research is on the case where $A$ in (2) is a rational integral matrix and on the question under what circumstances

$$A = S_1S_2, \ S_i = S_i^t, \ S_i \text{ with elements in } \mathbb{Z}.$$ 

For $n = 2$ a number of results have been obtained in [6], [7], e.g.:

1. If $\gcd(a_{21}, (a_{22} - a_{11}), a_{12}) = g$ then the discriminant of (5) and of (6) coincide apart from the factor $g^2$. Here the solutions $\alpha_1$, $\alpha_2$, $\alpha_3$; $\beta_1$, $\beta_2$, $\beta_3$ are assumed to be integral basis vectors for the lattice of all integral solutions of (4).

2. Let the characteristic polynomial of $A$ be $x^2 - m$, when $m \equiv 2, 3(4)$ and square free. Then (7) can only hold if the ideal class associated with $A$ by the relation

$$A \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = \alpha \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}$$

is of order 1 or 2 or 4. Here $\alpha$ is a characteristic root of $A$ and $\alpha_1$, $\alpha_2 \in \mathbb{Z}[\alpha]$ form a basis for an ideal $U$ in $\mathbb{Z}[\alpha]$.

3. Relation (7) holds for $A$ if and only if the form (5) represents a factor $d$ of $m$ (the discriminant of (5) is $4m$). In this case $-m/d$ is also represented so that in (7) one of the $S_i$ has determinant $d$, the other $-m/d$.

4. For an arbitrary $2 \times 2$ integral $A$ the following fact holds: relation (7) can be satisfied if and only if the form (5) can be transformed by a unimodular similarity to a form whose middle coefficient is trace $A$.

5. Every integral $2 \times 2$ matrix can be factored as in (7) when a suitable integral scalar matrix is added to it.

In the case of general $n$ and the characteristic polynomial $f(x)$ of $A$ irreducible the problem can be studied via a result obtained previously (see [4]) by several authors.

---

3 Since (4) defines a plane in 3-space the null-space of the binary quadratic form attached to $A$ can be regarded as the intersection of the plane with the cone $x_1x_3 - x_2^2 = 0$. 

---

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
If $A$ and $S$ in (1) are integral then $S = \text{trace } A \alpha$ where $\lambda \in \mathbb{Q}(\alpha)$, $\alpha$ a zero of $f(x)$ and $\alpha_1, \ldots, \alpha_n$ form a basis for the ideal $\mathfrak{U}$ constructed as in (8). From this follows that for $S$ to be integral it is necessary and sufficient that

$$\lambda \in (\mathfrak{U}^2)' = (\mathfrak{U} : \mathfrak{U}),$$

when $'$ denotes the complementary ideal.

For $S_1$ and $S_2$ to be integral in (7) it is necessary and sufficient that also

$$\lambda^{-1} \in (\mathfrak{U} : \mathfrak{U}).$$

The form in $n$ variables of degree $n$ mentioned at the start is connected with the norm form of an ideal (for this see Theorems 3, 4 in [3]). Some information concerning the order to which this ideal belongs can be seen from the greatest divisors of certain sets of elements in the matrix $A$.

One of the factors $S_i$ in (7) can be chosen unimodular if and only if the ideal class corresponding to $A$ in $\mathbb{Z}[\alpha]$ coincides with the ideal class corresponding to $A'$. If $\mathbb{Z}[\alpha]$ is the maximal order this is only possible if this ideal class is of order 1 or 2, (see [1], [2]).

REFERENCES


5. ———, Symmetric matrices and their role in the study of general matrices, Linear Algebra and Appl. 5 (1972), 147–159.


DEPARTMENT OF MATHEMATICS, CALIFORNIA INSTITUTE OF TECHNOLOGY, PASADENA, CALIFORNIA 91109