CLASSES OF MATRICES AND QUADRATIC FIELDS

OLGA TAUSSKY

1. Introduction. In a recent paper [1] a correspondence between classes of matrices with rational integral elements and ideal classes in algebraic number fields was discussed. This is now studied in more detail in the case of quadratic fields. In particular the ideal classes of order 2 are discussed and the significance of the sign of the norm of the fundamental unit in real quadratic fields is displayed in an example; further results in this connection will be published elsewhere.

For completeness the result of [1] is repeated:

Let $f(x) = 0$ be an irreducible algebraic equation of degree n with integral coefficients, α one of its algebraic roots, $A = (a_{ik})$ an $n \times n$ matrix with rational integers as elements which satisfies $f(x) = 0$, and S a matrix with rational integers as elements and determinant ± 1. It was shown that the matrix classes $S^{-1}AS$ are in one-to-one correspondence with the ideal classes in the ring generated by α. The correspondence can be expressed in the following way: If $\alpha_1, \cdots, \alpha_n$ is a module base for an ideal in the ring and A the matrix for which

$$\alpha(\alpha_1, \cdots, \alpha_n) = A(\alpha_1, \cdots, \alpha_n) \tag{1}$$

then the ideal class determined by $(\alpha_1, \cdots, \alpha_n)$ corresponds to the matrix class determined by A.

2. Inverse classes. Let m be a square-free positive or negative integer. Consider the quadratic field generated by $m^{1/2}$ or $(1/2)(-1 + m^{1/2})$ according as $m \equiv 2, 3\,(4)$ or $\equiv 1\,(4)$. The first result to be proved is the following.

THEOREM 1. *The inverse of an ideal class corresponds to the class determined by the transpose of the matrix class which corresponds to the ideal class.*

Proof. We treat the two cases separately.

(a) The case $m \equiv 2, 3\,(4)$. Here choose $\alpha = m^{1/2}$. Let α_1, α_2 be a module base for an ideal $\mathfrak{a}$. If

$$\alpha_1 = a + bm^{1/2}, \qquad \alpha_2 = c + dm^{1/2}$$

Received July 11, 1950.
Pacific J. Math. 1 (1951), 127-132.

then norm $(\alpha_1, \alpha_2) = |ad - bc|$. Put $ad - bc = \Delta$. On the other hand, norm $\mathfrak{a} = \alpha \cdot \alpha'$ when α' is the conjugate of α; hence,

$$\text{norm } \mathfrak{a} = [b^2m - a^2, \quad d^2m - c^2, \quad ac - bdm - \alpha(ad - bc), \quad ac - bdm + \alpha(ad - bc)].$$

In order to find the matrix

$$\begin{pmatrix} \lambda_1 & \lambda_2 \\ \mu_1 & \mu_2 \end{pmatrix}$$

which corresponds to the ideal $\mathfrak{a}$, we use the fact that

$$\alpha\alpha_1 = bm + a\alpha = \lambda_1(a + b\alpha) + \lambda_2(c + d\alpha),$$
$$\alpha\alpha_2 = dm + c\alpha = \mu_1(a + b\alpha) + \mu_2(c + d\alpha).$$

Hence,

$$\begin{pmatrix} \lambda_1 & \lambda_2 \\ \mu_1 & \mu_2 \end{pmatrix} = \begin{pmatrix} \frac{bdm - ac}{\Delta} & \frac{a^2 - b^2m}{\Delta} \\ \frac{d^2m - c^2}{\Delta} & \frac{ac - bdm}{\Delta} \end{pmatrix}.$$

The elements in this matrix are rational integers.

The ideal which corresponds to the transpose of this matrix is, by (1),

$$\left(\frac{ac - bdm}{ad - bc} - \alpha, \quad \frac{b^2m - a^2}{ad - bc} \right)$$

which is equivalent to

$$\mathfrak{b} = [ac - bdm - \alpha(ad - bc), \quad b^2m - a^2].$$

It will now be shown that this is an ideal inverse to $\mathfrak{a}$. For this purpose we show that the product $\mathfrak{ab}$ is a principal ideal, namely, the ideal $(ad - bc)\alpha_1$. For,

$$\mathfrak{ab} = \{[ac - bdm - \alpha(ad - bc)]\alpha_1, \quad [ac - bdm - \alpha(ad - bc)]\alpha_2, \quad (b^2m - a^2)\alpha_1, \quad (b^2m - a^2)\alpha_2\}.$$

The number $(b^2m - a^2)\alpha_2$ can be expressed in the following form:

$$-(bm^{1/2} + a)(a - bm^{1/2})(c + dm^{1/2}) = -\alpha_1[ac - bdm + \alpha(ad - bc)].$$

Similarly,

$$[ac - bdm - \alpha(ad - bc)]\,\alpha_2 = (d^2m - c^2)\,\alpha_1 .$$

Hence, it follows that

$$\alpha\beta = \alpha_1 \cdot \text{norm } \alpha .$$

(b) Case $m \equiv 1(4)$. Here we choose $\alpha = (1/2)(-1 + m^{1/2})$. Let

$$\alpha_1 = a + b\alpha = \frac{2a - b}{2} + \frac{bm^{1/2}}{2} ,$$

$$\alpha_2 = c + d\alpha = \frac{2c - d}{2} + \frac{dm^{1/2}}{2} .$$

Then

$$\text{norm } \alpha_1 = a(a-b) - b^2\,\frac{m-1}{4}, \quad \text{norm } \alpha_2 = c(c-d) - d^2\,\frac{m-1}{4} ,$$

$$\text{norm } \alpha = [\text{norm } \alpha_1 , \quad \text{norm } \alpha_2 , \quad a(c-d) - bd\,\frac{m-1}{4} + \alpha(bc - ad) ,$$

$$a(c-d) - bd\,\frac{m-1}{4} - \alpha(bc - ad)].$$

It follows that

$$\alpha\alpha_1 = b\,\frac{m-1}{4} + \alpha(a-b) = \lambda_1(a + b\alpha) + \lambda_2(c + d\alpha) ,$$

$$\alpha\alpha_2 = d\,\frac{m-1}{4} + \alpha(c-d) = \mu_1(a + b\alpha) + \mu_2(c + d\alpha) .$$

Hence,

$$\begin{pmatrix} \lambda_1 & \lambda_2 \\ \mu_1 & \mu_2 \end{pmatrix} = \begin{pmatrix} \dfrac{bd\,\frac{m-1}{4} - c(a-b)}{\Delta} & \dfrac{d^2\frac{m-1}{4} - c(c-d)}{\Delta} \\ \dfrac{a(a-b) - b^2\,\frac{m-1}{4}}{\Delta} & \dfrac{a(c-d) - bd\,\frac{m-1}{4}}{\Delta} \end{pmatrix} .$$

Again, all the numbers in this matrix are rational integers.

The ideal which corresponds to the transposed matrix is equivalent to:

$$\mathfrak{b} = \left[a(c-d) - bd\,\frac{m-1}{4} - \alpha(ad-bc)\,, \qquad a(a-b) - b^2\,\frac{m-1}{4} \right].$$

The product ideal $\mathfrak{a}\mathfrak{b}$ is again shown to be the principal ideal $(ad-bc)\alpha_1$. For it is

$$\left\{(\alpha_1 \text{ norm } \alpha_1\,, \qquad \alpha_2 \text{ norm } \alpha_1, \qquad \alpha_1\left[a(c-d) - bd\,\frac{m-1}{4} - \alpha(ad-bc)\right],\right.$$

$$\left.\alpha_2\left[a(c-d) - bd\,\frac{m-1}{4} - \alpha(ad-bc)\right]\right\}.$$

We have

$$\alpha_2 \text{ norm } \alpha_1 = (a+b\alpha)(a+b\alpha')(c+d\alpha)$$

where α' is the conjugate of α. Further,

$$(a+b\alpha')(c+d\alpha) = \frac{[2a+b(-1-m^{1/2})][2c+d(-1+m^{1/2})]}{4}$$

$$= a(c-d) - bd\,\frac{m-1}{4} + \alpha(ad-bc)\,.$$

Similarly,

$$\alpha_2\left[a(c-d) - bd\,\frac{m-1}{4} - \alpha(ad-bc)\right] = \alpha_1 \text{ norm } \alpha_2\,.$$

This shows that again, $\mathfrak{a}\mathfrak{b} = \alpha_1 \text{ norm } \mathfrak{a}$.

3. Classes of order two. From Theorem 1 it follows that a matrix which corresponds to an ideal class of order 2 is equivalent to its transpose. The question arises, when does the class to which this matrix belongs contain a symmetric matrix? A result in this direction is the following.

THEOREM 2. *A matrix class which corresponds to an ideal class of order two contains a symmetric matrix if and only if every matrix in the class is transformed into its transpose by a unimodular matrix of the form XX'. In particular the transforming matrix must be of determinant $+1$.*

Proof. Let A be a matrix equivalent with its transpose; that is,

$$A' = SAS^{-1}$$

when S is unimodular. Let T also be unimodular and assume that $T^{-1}AT$ is symmetric. We then have

$$T^{-1}AT = T'A'T'^{-1}$$

or

$$T'^{-1}T^{-1}ATT' = A' .$$

Hence, it is possible to transform A into its transpose by a matrix of the form XX'. Conversely, if

$$A' = X'^{-1}X^{-1}AXX'$$

we have

$$X'A'X'^{-1} = X^{-1}AX .$$

Hence $X^{-1}AX$ is symmetric.

The question arises, are both cases possible, the one when the matrix class contains symmetric matrices and the one when it does not? Both cases, in fact, are possible and it can even happen that the same field contains ideal classes of order 2, some of which correspond to symmetric matrices, while others do not. An example is the field generated by $(410)^{1/2}$. An ideal of order 2 in this field is $[7, 19 + (410)^{1/2}]$, and a matrix which corresponds to it is

$$\begin{pmatrix} -19 & 7 \\ 7 & 19 \end{pmatrix} ,$$

which is clearly symmetric. Another ideal of order 2 in the same field is the ideal $[2, 20 + (410)^{1/2}]$, a corresponding matrix being

$$\begin{pmatrix} -20 & 2 \\ 5 & 20 \end{pmatrix} .$$

Any matrix which transforms the latter into its transpose is of the form

$$\begin{pmatrix} \dfrac{-40b + 5d}{2} & b \\ b & d \end{pmatrix}$$

where b, d are parameters. In order to have integral coefficients we put $d = 2d'$. The matrix will then be

$$\begin{pmatrix} -20b + 5d' & b \\ b & 2d' \end{pmatrix} .$$

This will be unimodular if

$$-40bd' + 10d'^2 - b^2 = 410d'^2 - (b + 20d')^2 = \pm 1 .$$

This equation for +1 is impossible, since the fundamental unit of the field generated by $(410)^{1/2}$ has the norm +1. Hence, the matrix class which corresponds to this ideal does not contain any symmetric matrix.

A symmetric matrix can correspond only to ideals in real fields since such a matrix can have only real characteristic roots. It can further be seen easily that, in this case, m has to be a sum of two squares.

Reference

1. Olga Taussky, *On a theorem of Latimer and MacDuffee*, Canadian J. Math. **1** (1949), 300-302.

National Bureau of Standards