ON MATRIX CLASSES CORRESPONDING TO AN IDEAL AND ITS INVERSE

BY OLGA TAUSSKY[1]

1. It is known (Latimer and MacDuffee [1], Taussky [2], Zassenhaus [3], Reiner [4]), that there is a 1–1 correspondence between classes of $n \times n$ matrices A of rational integers and ideal classes. The matrix A is assumed to be a zero of an irreducible polynomial $f(x)$ of degree n with rational integral coefficients and first coefficient 1. The class associated with A consists of all matrices $S^{-1}AS$ where S runs through all unimodular matrices with rational integral coefficients. Let α be an algebraic number root of $f(x) = 0$. Then the 1–1 correspondence between the matrix classes and the ideal classes may be described as follows: If $(\alpha_1, \cdots, \alpha_n)$ is a modular basis for an ideal $\mathfrak{a}$ in the ring generated by α and $\alpha(\alpha_1, \cdots, \alpha_n)' = A(\alpha_1, \cdots, \alpha_n)'$, then the ideal class determined by $\mathfrak{a}$ corresponds to the matrix class determined by A. In what follows we assume that the numbers $1, \alpha, \alpha^2, \cdots$ form an integral basis in the field $R(\alpha)$.

It was further shown (Taussky [5], [6]) that for quadratic fields the matrix class generated by the transpose of A corresponds to the inverse class. It is now shown that this is always true. This fact is established in two different ways, once directly, secondly by using a known lemma (Hasse [7], pp. 327–328). Both proofs make use of the so-called complementary ideal (see Dedekind [8], pp. 374–376; see also Hecke [9], pp. 131–133).

It is easily seen directly that both the companion matrix C of $f(x)$ and its transpose correspond to the principal class in $R(\alpha)$. Hence

$$C' = S^{-1}CS$$

where S is unimodular. The matrix S can be constructed explicitly.

It is further shown that the matrix classes defined by unimodular matrices S with $|S| = 1$ coincide with the classes defined by $|S| = \pm 1$ if and only if the field has a unit ε with norm $\varepsilon = -1$.

In [5], [6] the matrix classes which correspond to ideal classes of order 2 in a quadratic field were studied. The transpose of a matrix in such a class belongs to the same class. It is now shown that such a class contains a symmetric matrix if the fundamental unit ε has norm $\varepsilon = -1$. This can also be regarded as a special case of a theorem proved by Faddeev [10] from a different point of view.

2. THEOREM 1.[2] *Let the matrix A correspond to the ideal class determined*

Received July 27, 1956.

[1] The preparation of this paper was sponsored (in part) by the Office of Naval Research.

[2] The author is indebted to E. Artin for a helpful remark.

by the ideal $\mathfrak{a} = (\alpha_1, \cdots, \alpha_n)$ *and let the transpose* A' *correspond to the ideal* $\mathfrak{b} = (\beta_1, \cdots, \beta_n)$. *Then* $\mathfrak{b}$ *belongs to the inverse class of* $\mathfrak{a}$.

First proof. We first prove that the numbers β_i are proportional to a set of numbers γ_i in the same field such that trace $(\alpha_i \gamma_k) = \delta_{ik}$. This implies (see [9]) that the ideal $(\gamma_1, \cdots, \gamma_n) = 1/\mathfrak{a}\mathfrak{d}$ where $\mathfrak{d}$ is the so-called different ideal of the field. Since $1, \alpha, \cdots, \alpha^{n-1}$ form an integral basis $\mathfrak{d} \sim 1$. Hence $\mathfrak{b} \sim \mathfrak{a}^{-1}$ follows.

In order to find the numbers γ_i, denote the conjugates of $\alpha_i = \alpha_i^{(1)}$ by $\alpha_i^{(k)}$ and the matrix $(\alpha_k^{(i)})$ by Δ, further the (i, k) cofactor of Δ by Δ_{ik}.

The numbers $\alpha_1, \cdots, \alpha_n$ form an eigenvector of A with respect to α. It is known that an eigenvector is orthogonal to those eigenvectors of A' which do not correspond to α. Similarly $(\beta_1, \cdots, \beta_n)$ forms an eigenvector of A' orthogonal to the eigenvectors of A which do not correspond to α. Hence

$$\beta_1 \alpha_1^{(i)} + \beta_2 \alpha_2^{(i)} + \cdots + \beta_n \alpha_n^{(i)} = 0, \qquad i = 2, \cdots, n.$$

From this it follows that the two sequences $\beta_1, \cdots, \beta_n$ and $\gamma_i = \Delta_{i1}/|\Delta|$, $i = 1, \cdots, n$, are proportional. It can be shown that the numbers γ_i lie in the original field $R(\alpha)$. For, they are invariant under the permutations of the Galois group which leave that field invariant. For, such a permutation of the Galois group will only alter Δ_{i1} and $|\Delta|$ by the same factor ± 1 which cancels out. For the conjugates of γ_i we have

$$\gamma_i^{(k)} = \Delta_{ik}/|\Delta|, \qquad i = 1, \cdots, n, \quad k = 1, \cdots, n$$

since the rows of Δ_{ik} consist of the conjugates of the rows of Δ_{i1} and since a possible permutation will affect Δ_{ik} and $|\Delta|$ simultaneously.

We therefore have

$$\text{trace } (\alpha_i \gamma_k) = \sum_{j=1}^{n} \alpha_i^{(j)} \gamma_k^{(j)} = \sum_{j=1}^{n} \alpha_i^{(j)} \Delta_{kj}/|\Delta| = \delta_{ik}.$$

Second proof. We use the following lemma (see [7]):

LEMMA. *Let* $\Delta = (\alpha_k^{(i)})$ *as before. Then* $\Delta = \Delta'^{-1}$ *is again of the form* $(\tilde{\alpha}_k^{(i)})$, *and the numbers* $\tilde{\alpha}_1, \cdots, \tilde{\alpha}_n$ *form a basis of the ideal* $1/\mathfrak{a}\mathfrak{d}$.

From the definition of the correspondence we have

$$A \begin{pmatrix} \alpha_1^{(i)} \\ \vdots \\ \alpha_n^{(i)} \end{pmatrix} = \alpha^{(i)} \begin{pmatrix} \alpha_1^{(i)} \\ \vdots \\ \alpha_n^{(i)} \end{pmatrix}, \qquad i = 1, \cdots, n.$$

This implies

$$\Delta^{-1} A \Delta = \begin{pmatrix} \alpha^{(1)} & & & \\ & \alpha^{(2)} & & \\ & & \ddots & \\ & & & \alpha^{(n)} \end{pmatrix}$$

where the right hand matrix is a diagonal matrix. Taking the transpose of both sides we have

$$\Delta' A' \Delta'^{-1} = \begin{pmatrix} \alpha^{(1)} & & & \\ & \alpha^{(2)} & & \\ & & \ddots & \\ & & & \alpha^{(n)} \end{pmatrix}.$$

Hence, in virtue of the lemma, the ideal which corresponds to A' is equivalent to $1/\mathfrak{a}\mathfrak{d}$.

THEOREM 2. *The companion matrix of $f(x)$ and its transpose both correspond to the principal class in $R(\alpha)$.*

Proof. This follows immediately from Theorem 1. However, a more elementary direct proof can be given. This proof can also be used to give an elementary demonstration for the fact that $\mathfrak{d} \sim 1$ in our case. Let $f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n$. The companion matrix is

$$C = \begin{pmatrix} 0 & 1 & 0 & \cdot & 0 & 0 \\ 0 & 0 & 1 & \cdot & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdot & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \cdot & \cdot & -a_{n-1} \end{pmatrix}.$$

It has the eigenvalue α with corresponding eigenvector $(1, \alpha, \cdots, \alpha^{n-1})$. It is also easily checked that C' has as eigenvector corresponding to α the vector

$$(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1, \alpha^{n-2} + a_{n-1}\alpha^{n-3} + \cdots + a_2, \cdots, \alpha + a_{n-1}, 1)$$

which is obtained from $(1, \alpha, \cdots, \alpha^{n-1})$ by a unimodular substitution.

3. For ideal classes the concept of class division in the "large sense" and class division in the "narrow sense" is used. Similarly, but in a weaker sense, we have two possibilities for the definition of matrix class, one by assuming $|S| = +1$, the other by assuming that $|S| = \pm 1$. The following theorem shows when the two definitions coincide.

THEOREM 3. *The two definitions of matrix class coincide if and only if the field $R(\alpha)$ contains a unit ε of* norm $\varepsilon = -1$.

Proof. We first establish two lemmas.

LEMMA 1. *Let A and B be $n \times n$ matrices with rational integral coefficients which commute, and let the characteristic polynomial of A be an irreducible polynomial. Then B is a polynomial in A with rational coefficients.*

Proof. That B is a polynomial in A follows from the fact that the characteristic roots of A are different, see e.g. [11]. This polynomial can be chosen of

degree $<n$. In order to prove that the coefficients are rational we use the fact that a pair of commutative matrices have a common eigenvector (see e.g. [12]). Let x be this vector, and α, β the corresponding eigenvalues. We then have

$$Ax = \alpha x, \qquad Bx = \beta x.$$

Since the vector x can be chosen in the field $R(\alpha)$, generated by α, the number β also lies in $R(\alpha)$. Hence β is a polynomial in α of degree $<n$ with rational coefficients which are uniquely determined. It must coincide with the above polynomial.

From the proof of lemma 1 we obtain immediately the following other lemma:

LEMMA 2. *Let A and B be matrices with rational integral coefficients which commute. Let the characteristic polynomial of A be an irreducible polynomial $f(x)$ whose zero α forms with its powers an integral basis in the ring of algebraic integers in $R(\alpha)$. Then B is a polynomial in A with rational integral coefficients.*

We now return to the proof of Theorem 3. Assume that the two definitions coincide. Then to a given matrix S with $|S| = -1$ there must exist a matrix T with $|T| = 1$ such that $S^{-1}AS = T^{-1}AT$. This implies

$$TS^{-1}AST^{-1} = A,$$

i.e. there exists a matrix $X = ST^{-1}$ with rational integral elements and determinant -1 which commutes with A. Since A has distinct characteristic roots, X is a polynomial in A, $p(A)$. By Lemmas 1 and 2 the coefficients of this polynomial are rational integers. Since the eigenvalues of $p(A)$ are $p(\alpha)$, it follows that the polynomial $p(\alpha)$ is a unit ε in $R(\alpha)$ of norm $\varepsilon = -1$.

Conversely, if there is such a unit in $R(\alpha)$, then it is a polynomial in α with integral coefficients. The corresponding polynomial in A is a matrix Y which commutes with A and has determinant -1. If then S is a unimodular matrix with $|S| = -1$, then

$$S^{-1}AS = S^{-1}Y^{-1}AYS,$$

hence

$$S^{-1}AS = T^{-1}AT$$

where $T = YS$ and $|T| = 1$.

4. If the ideal class is of order 2, the transposed matrix lies in the same class as the original matrix. In some cases the matrix class which corresponds to an ideal class of order 2 can even contain a symmetric matrix.

THEOREM 4. *Let m be a square free positive integer. Let the fundamental unit of the field $R(\sqrt{m})$ be of norm -1. Then every class of matrices which corresponds to an ideal class of order 2 in this field contains a symmetric matrix.*

Proof. Let $S^{-1}AS$ be a matrix class which corresponds to an ideal class of

order 2, and let $T^{-1}AT = A'$. In [5] it was shown that the class $S^{-1}AS$ contains a symmetric matrix if T can be chosen of the form XX' where X is again a matrix of integers. This is certainly the case if $|T| = 1$ since in this case T can also be assumed to be positive definite, and since it is known that a positive definite unimodular 2×2 matrix is of the form XX'. Theorem 4 then follows from Theorem 3.

Remark. S. Chowla communicated to me the following simple proof for the fact that a positive definite 2×2 matrix of integers $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ with $ac - b^2 = 1$ can be written in the form $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$ where $\alpha, \beta, \gamma, \delta$ are integers. Assume also that $\alpha\delta - \beta\gamma = 1$. Factorize $b + i$ into its prime factors in the Gaussian field. Let $\gamma + \delta i$ be the product of those prime factors of c (with repetition) which occur in $b + i$. Let $\alpha - \beta i$ be the product of the remaining factors of $b + i$. Then

$$b + i = (\alpha - \beta i)(\gamma + \delta i),$$

hence

$$b = \alpha\gamma + \beta\delta, \tag{1}$$

$$1 = \alpha\delta - \beta\gamma. \tag{2}$$

Since $b + i$ is not divisible by a rational prime, $\gamma + \delta i$ cannot be divisible by a rational prime. This implies that $\gamma^2 + \delta^2 \mid c$. This again implies that $\gamma^2 + \delta^2 = c$, for

$$\text{norm } (b + i) = b^2 + 1 = ac$$

and $\gamma + \delta i$ is the largest common divisor of $b + i$ and c. Hence

$$a = \alpha^2 + \beta^2, \tag{3}$$

$$c = \gamma^2 + \delta^2. \tag{4}$$

The relations (1), (2), (3), (4) imply that

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}.$$

References

1. C. G. Latimer and C. C. MacDuffee, *A correspondence between classes of ideals and classes of matrices*, Ann. of Math., vol. 34 (1933), pp. 313–316.
2. Olga Taussky, *On a theorem of Latimer and MacDuffee*, Canadian J. Math., vol. 1 (1949), pp. 300–302.
3. H. Zassenhaus, *Neuer Beweis der Endlichkeit der Klassenzahl bei unimodularer Äquivalenz endlicher ganzzahliger Substitutionsgruppen*, Abh. Math. Sem. Univ. Hamburg, vol. 12 (1938), pp. 276–288.
4. I. Reiner, *Integral representations of cyclic groups of prime order*, to appear in Proc. Amer. Math. Soc., vol. 8 (1957).
5. Olga Taussky, *Classes of matrices and quadratic fields*, Pacific J. Math., vol. 1 (1951), pp. 127–131.

6. ———, *Classes of matrices and quadratic fields, II*, J. London Math. Soc., vol. 27 (1952), pp. 237–239.
7. H. Hasse, *Zahlentheorie*, Berlin, 1949.
8. R. Dedekind, *Über die Diskriminanten endlicher Körper*, Gesammelte mathematische Werke, vol. I, Braunschweig, 1930.
9. E. Hecke, *Theorie der algebraischen Zahlen*, Leipzig, 1923.
10. D. K. Faddeev, *On the characteristic equations of rational symmetric matrices*, Dokl. Akad. Nauk SSSR (N.S.), vol. 58 (1947), pp. 753–754.
11. H. L. Hamburger and M. E. Grimshaw, *Linear transformations in n-dimensional vector space*, Cambridge, 1951.
12. M. P. Drazin, J. W. Dungey, and K. W. Gruenberg, *Some theorems on commutative matrices*, J. London Math. Soc., vol. 26 (1951), pp. 221–228.

National Bureau of Standards
Washington, D. C.