Classes of Matrices and Quadratic Fields*

EDWARD A. BENDER
Harvard University
Cambridge, Massachusetts

Communicated by Alan J. Hoffman

1. INTRODUCTION

Let $A, B, C, \ldots$ lie in $\mathbf{Z}_2$, the 2×2 matrices over the rational integers. Similarity under integral unimodular transformations defines equivalence classes. Taussky [5, 6, 7] studied the structure of these classes, with special attention to those containing symmetric matrices. We shall determine

(i) the number of symmetric matrices in each equivalence class,
(ii) the transformations relating the symmetric matrices in a class,
(iii) the structure of the symmetric matrices in a class.

Let $p(x)$ be an irreducible monic quadratic polynomial over $\mathbf{Z}$, the rational integers. Let θ be a root of $p = 0$. A correspondence has been established [4, 5] between classes of ideals of $\mathbf{Z}[\theta]$ and classes of roots of $p = 0$ in $\mathbf{Z}_2$. It is given by

$$\mathscr{C}(a) \leftrightarrow \mathscr{C}(A), \tag{1}$$

where $A\vec{\alpha} = \theta\vec{\alpha}$, the components α_1, α_2 of $\vec{\alpha}$ are in $Q(\theta)$, and

$$a = \mathbf{Z}\alpha_1 + \mathbf{Z}\alpha_2.$$

The map $q(A) \to q(\theta)$ defines a natural isomorphism between $Q(A)$ and $Q(\theta)$, where $q(x) \in Q[x]$. Define $R(A)$ under this map by

$$Q(A) \cap \mathbf{Z}_2 \xrightarrow{\sim} R(A). \tag{2}$$

* I should like to thank my advisor, Dr. Olga Taussky Todd, for her aid on my thesis [1]. This is a new presentation of the last chapter.

Linear Algebra and Its Applications 1, 195–201 (1968)

It is easily seen that $R(A)$ depends only on the class of A: if T is integral and unimodular, then $q(A) \in \mathbf{Z}_2$ if and only if

$$q(TAT^{-1}) = Tq(A)T^{-1} \in \mathbf{Z}_2.$$

Since symmetric matrices have real roots, *we shall assume that θ is real.*

2. THE NUMBER

We now determine the classes containing symmetric matrices (see [7]) and the number in each such class. Let a' be the complement of the ideal a. (For details see [3, p. 41].) It is known [7] that $\mathscr{C}(a') \leftrightarrow \mathscr{C}(A')$ when (1) holds.

THEOREM 1. *Let $\mathscr{C}(A) \leftrightarrow \mathscr{C}(a)$. Then $\mathscr{C}(A)$ contains a symmetric matrix if and only if $a = \lambda a'$ for some λ with $N\lambda > 0$. If $\mathscr{C}(A)$ contains a symmetric matrix and if $R(A)$ has (does not have) a unit of norm -1, then $\mathscr{C}(A)$ contains 4 (8) symmetric matrices.*

Proof. Apply [2, Theorem 6] with $n = 2$. If $N\lambda > 0$, then λ or $-\lambda$ is totally positive. In the notation of [2], the number of symmetric matrices is $4[U^N : U^2]$, where U^N is the group of totally positive units in $R(A)$ and U^2 is the group of squares of units in $R(A)$. Clearly $[U^N : U^2] =$ 1 if $R(A)$ has a unit of norm -1, and 2 otherwise.

COROLLARY. *If $R(A)$ contains a unit of norm -1, then $\mathscr{C}(A)$ contains a symmetric matrix if and only if $A' \in \mathscr{C}(A)$.*

Proof. $A' \in \mathscr{C}(A)$ if and only if $a' \in \mathscr{C}(a)$ by the remark preceding the theorem. Let $a = \lambda a'$. If $N\lambda < 0$, replace λ by $\lambda\eta$ where $\eta \in R(A)$ is a unit of norm -1.

COROLLARY [6]. *If $\mathbf{Z}[\theta]$ is the ring of integers in $Q(\theta)$, then $\mathscr{C}(A) \leftrightarrow \mathscr{C}(a)$ contains a symmetric matrix if and only if $a^2 = (\mu)$ for some $\mu \in Q(\theta)$ with $N\mu < 0$.*

Proof. The different of $Q(\theta)$ is $(p'(\theta))$ where p is the monic quadratic polynomial with θ as a zero. Hence $a = \lambda a'$ is equivalent to $a^2 = (\lambda p'(\theta))$. Since $Np'(\theta) < 0$, the corollary is proved.

3. THE SIMILARITY TRANSFORMATIONS

The similarity transformations relating the symmetric matrices in a given class are closely related to the gaussian integers $\mathbf{Z}[i]$ and certain quadratic diophantine equations.

It is well known that every integral domain which is a quadratic, integral extension of $\mathbf{Z}$ is principal. Hence we may write

$$R(A) = \mathbf{Z}[\omega = (1 + \sqrt{m})/k], \tag{3}$$

where (2) defines $R(A)$ and $m \in \mathbf{Z}$ and $k = 1$ or 2. Under the natural isomorphism $Q(A) \cong Q(\theta)$ we have

$$\begin{pmatrix} -b & a \\ a & b \end{pmatrix} \to \sqrt{m} \qquad \text{for some} \quad a, b \in \mathbf{Z}. \tag{4}$$

The *gaussian integer associated with* A is

$$\gamma(A) = a + bi.$$

LEMMA. *Let A and B be equivalent symmetric matrices. For some $\lambda, \mu \in \mathbf{Z}[i]$ we have*

$$\gamma(A) = \lambda\mu \qquad \textit{and} \qquad \gamma(B) = \lambda\bar{\mu}. \tag{5}$$

The values of λ and μ are unique up to sign.

Proof. Let $\alpha = \gamma(A)$ and $\beta = \gamma(B)$. Since $R(A) = R(B)$, we have

(i) $N(\alpha) = m = N(\beta)$,
(ii) $\alpha \equiv i (\mathrm{mod}\ 2)$ if and only if $\beta \equiv i (\mathrm{mod}\ 2)$,

since these are equivalent to $k = 2$ in (3). From (*i*) and the structure of $\mathbf{Z}[i]$, it follows that there are $\lambda, \mu \in \mathbf{Z}[i]$ such that $\alpha = \lambda\mu$ and $\beta = i^n\lambda\bar{\mu}$ for some $n \in \mathbf{Z}$. By the definition of $\alpha = \gamma(A)$, it follows that no rational prime divides α. Applying this to the prime 2 and using (i) and (ii), we get $\alpha \equiv \beta (\mathrm{mod}\ 2)$. However, $\lambda\mu \equiv \lambda\bar{\mu} (\mathrm{mod}\ 2)$. These are compatible if and only if n is even or $\alpha \equiv 1 + i (\mathrm{mod}\ 2)$. In the latter case $1 + i$ divides λ or μ, and moving it from one of λ, μ to the other changes the parity of n. Hence we may assume $n = 0$ or 2. If $n = 2$, replace λ by λi and μ by $-\mu i$.

We now prove uniqueness. Assume $\alpha = \lambda_1\mu_1 = \lambda_2\mu_2$ and $\beta = \lambda_1\bar{\mu}_1 = \lambda_2\bar{\mu}_2$. Then

$$\rho = \mu_2/\mu_1 = \lambda_1/\lambda_2 = \bar{\mu}_2/\bar{\mu}_1 = \bar{\rho}.$$

Hence ρ is real. We may write $\rho = c/d$ where $c, d \in \mathbf{Z}$ and $gcd(c, d) = 1$. Suppose $|c| > 1$. Then a rational prime divides $\lambda_1 = c\lambda_2/d$ and hence α, which we have noted is impossible. Thus $|c| = |d| = 1$.

The matrix representation of the complex number $x + iy$ is

$$K(x + iy) = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}.$$

If

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

then (4) becomes $PK(\gamma(A)) \to \sqrt{m}$. We also have $K(\alpha)P = PK(\bar{\alpha})$.

THEOREM 2. *Let $A \neq B$ be symmetric and equivalent. A transformation T satisfies $TA = BT$ if and only if it has the form*

$$T = xK(\mu) + yPK(\lambda), \tag{6}$$

where x and y are scalars and (5) *defines λ and μ.*

Proof. Given A and B, choose λ and μ. Instead of A and B in $TA = BT$ we may consider $PK(\gamma(A))$ and $PK(\gamma(B))$ since they also generate $R(A)$ and $R(B)$. We have

$$\begin{aligned} K(\mu)PK(\gamma(A)) &= PK(\bar{\mu})K(\lambda\mu) \\ &= PK(\lambda\bar{\mu})K(\mu) \\ &= PK(\gamma(B))K(\mu) \end{aligned}$$

and

$$\begin{aligned} PK(\lambda)PK(\gamma(A)) &= PK(\lambda)K(\bar{\mu})PK(\lambda) \\ &= PK(\gamma(B))PK(\lambda). \end{aligned}$$

Hence any T of the form (6) works. Conversely, given T choose x and y so that

$$W = T - xK(\mu) - yPK(\lambda)$$

has as many zero entries as possible. It has at least two zero entries since $K(\mu)$ and $PK(\lambda)$ are linearly independent. The equation

$$WPK(\gamma(A)) = PK(\gamma(B))W$$

can be used to show that $W = 0$.

There are four rather trivial choices for the pair (λ, μ), namely $(\alpha, 1)$, $(1, \alpha)$, $(i\alpha, -i)$, and $(i, -i\alpha)$. These correspond to $T = I, P, K(i)$, and $PK(i)$ and also to $\gamma(B) = \alpha, \bar{\alpha}, -\alpha$, and $-\bar{\alpha}$.

The determinant of (6) is easily seen to be $x^2N\mu - y^2N\lambda$. This together with Theorems 1 and 2 enables us to deduce a result in diophantine analysis:

THEOREM 3. *The diophantine equation*

$$wx^2 - \frac{m}{w}y^2 = k^2, \tag{7}$$

where m and k satisfy (3) *for some symmetric A, has solutions for precisely two positive divisors w of m.*

Proof. For any solution of (7) choose λ and μ so that $N\lambda = m/w$ and $N\mu = w$ and $\lambda\mu = \gamma(A)$. Let

$$T = \frac{1}{k}(xK(\mu) + yPK(\lambda)).$$

Then $\det T = \pm 1$. Clearly $kT \in \mathbf{Z}_2$. Assume $k = 2$. As noted in the proof of the lemma, $\lambda\mu \equiv i (\mathrm{mod}\ 2)$. Hence $\lambda \equiv i\mu (\mathrm{mod}\ 2)$. By (7) we have $x \equiv y (\mathrm{mod}\ 2)$. These congruences can be used to show that $T \in \mathbf{Z}_2$.

We could replace the pair (λ, μ) by any of (μ, λ), $(i\lambda, -i\mu)$, and $(i\mu, -i\lambda)$. By Theorem 2 these all lead to distinct values for B. The same B's are obtained when w is replaced by m/w, so there is a potential pairing of solutions to (7). We now use Theorem 1.

(i) If $R(A)$ has a unit of norm -1, then there are four possible values for B (including A itself). Thus the solutions of (7) occur with $w = 1$ and m (the latter due to the unit of norm -1).

(ii) If $R(A)$ has no unit of norm -1, then there is a solution for some w with $1 < w < m$. The potential pairing of solutions (w and m/w) cannot occur as we now show. Construct $T(w)$ using (λ, μ). Then we have

$$T(w)AT(w)^{-1} = B = T(m/w)AT(m/w)^{-1}.$$

Hence $V = T(m/w)T(w)^{-1}$ commutes with A. It is well known that this implies that V is a polynomial in A. Since V is integral and unimodular, it is the image of a unit in $R(A)$. On the other hand, $\det T(w) = -\det T(m/w)$ so $\det V = -1$.

4. THE MATRICES IN A CLASS

We assume one symmetric matrix is known and we wish to find the rest in its class. If w in (7) can be found, then four pairs (λ, μ) are determined. By (5) we can determine four symmetric matrices similar to A. (As remarked after Theorem 2, if one of these is B and if $\gamma(B) = \beta$, then the other three correspond to $\bar{\beta}$, $-\beta$, and $-\bar{\beta}$.) This procedure avoids the determination of T. Since m and k depend only on $R(A)$, the same is true of w, so it is natural to define

$$\sigma(\omega) = \{w, m/w\},$$

where $R(A) = \mathbf{Z}[\omega]$ and $w > 1$ is a solution of (7). Using the continued fraction approach to ideal equivalence, it is feasible to construct a large table of σ using a digital computer. Some properties of σ are given below.

THEOREM 4. *If all the σ's mentioned are defined, then*

(i) $1 \in \sigma(\omega)$ *if and only if* $\mathbf{Z}[\omega]$ *has a unit of norm* -1;
(i′) *if* $1 \in \sigma(l\omega)$, *then* $1 \in \sigma(\omega)$;
(ii) $\sigma(\sqrt{m}) = \sigma((1 + \sqrt{m})/2)$;
(iii) *if* $l|m$ *either of* $\sigma(\omega)$ *and* $\sigma(l\omega)$ *determines the other*;
(iv) *if* $\sigma(\omega) = \{a, b\}$ *and* p *is an odd prime, then* $\sigma(p\omega)$ *is one of* $\{ab, p^2\}$, $\{a, bp^2\}$, *and* $\{ap^2, b\}$;
(v) *if* p *is an odd prime divisor of* m, *then that element of* $\sigma(\omega)$ *which is prime to* p *is also a quadratic residue of* p.

Proof. (i) This follows from considerations in the proof of Theorem 3.

(ii) Any solution to (7) for $k = 1$ yields an obvious solution for $k = 2$. By Theorem 3, this determines all values of w for $k = 2$.

(iii) If $1 \in \sigma(l\omega)$, we are done by (i′). Induct on l. If $2|l$ we are done by (ii). Let $p|l$ be an odd prime. Assume $1 \notin \sigma(l\omega) = \{a, b\}$. We have $p^3|l^2m$ and, since $gcd(a, b) = 1$ or 2, $p^3|a$ or b. We can combine a factor of p^2 with x^2 or y^2 in (7). This produces, say, a' and b' *neither of which is* 1. Hence $\sigma(l\omega/p) = \{a', b'\}$. The process is reversible since we have just shown that $1 \notin \sigma(\omega l)$ implies $1 \notin \sigma(\omega)$.

(iv) Like (iii), but the conclusion that $1 \notin \{a', b'\}$ does not hold.

(v) Reduce (7) modulo p. Since m must be a sum of two squares ($m = N\gamma(A)$), we have that -1 is a quadratic residue of p.

By an elementary but involved elimination of cases relying on Theorem 4, it can be shown [1, pp. 95–97] that if p, q, and r are primes congruent to 1 modulo 4 and if $\sigma(\omega)$ is defined, then $\sigma(pq\omega)$, $\sigma(pr\omega)$, and $\sigma(qr\omega)$ determine $\sigma(pqr\omega)$. No result of this form holds for two primes: the following examples were found on an IBM 7094.

$$\sigma(\sqrt{13 \cdot 17}) = \{13, 17\} \qquad \sigma(\sqrt{5 \cdot 41}) = \{5, 41\}$$

$$\sigma(5\sqrt{13 \cdot 17}) = \{5^2, 13 \cdot 17\} \qquad \sigma(13\sqrt{5 \cdot 41}) = \{13^2, 5 \cdot 41\}$$

$$\sigma(37\sqrt{13 \cdot 17}) = \{37^2, 13 \cdot 17\} \qquad \sigma(17\sqrt{5 \cdot 41}) = \{17^2, 5 \cdot 41\}$$

$$\sigma(5 \cdot 37\sqrt{13 \cdot 17}) = \{5^2 37^2, 13 \cdot 17\} \qquad \sigma(13 \cdot 17\sqrt{5 \cdot 41}) = \{17^2, 13^2 5 \cdot 41\}$$

REFERENCES

1 E. Bender, Symmetric representations of an integral domain over a subdomain, doctoral thesis, California Institute of Technology, 1966.

2 E. Bender, Classes of matrices over an integral domain, *Illinois J. Math.* **11**(1967), 697–702.

3 S. Lang, *Algebraic numbers*, Addison-Wesley, Reading Massachusetts, 1964.

4 C. Latimer and C. MacDuffe, A correspondence between classes of ideals and classes of matrices. *Ann. Math.* 34(1933), 313–316.

5 O. Taussky, Classes of matrices and quadratic fields, *Pacific J. Math.* 1(1951), 127–132.

6 O. Taussky, Classes of matrices and quadratic fields II, *J. London Math. Soc.* 27(1952), 237–239.

7 O. Taussky, On matrix classes corresponding to an ideal and its inverse, *Illinois J. Math.* 1(1957), 108–113.