# CLASSES OF MATRICES OVER AN INTEGRAL DOMAIN

BY
EDWARD A. BENDER[1]

## 1. Introduction

It is known [8], [10] that there is a one-to-one correspondence between (i) classes of matrices of rational integers with a given irreducible characteristic polynomial $p(x)$ and (ii) classes of ideals in $\mathbf{Z}[x]/(p(x))$. We will generalize this correspondence and some of its properties. The existence of symmetric matrices in a class has been studied [4], [12], but not the number. We shall take up this question. The application of our results to the rational integer case will be discussed.[2]

## 2. Basic concepts

Let $\Delta$ and $D$ be integral domains with quotient fields $G$ and $F$ such that

(1) $\Delta \supset D$,
(2) $G$ is a separable extension of $F$,
(3) $[G:F] = n < \infty$.

We may write $G = F(\theta)$ for some $\theta \in \Delta$. This notation will be fixed throughout the paper.

DEFINITION. A *representation* of $\Delta$ over $D$ is a ring isomorphism $\Phi$ of $\Delta$ onto a subring of $D_n$, the $n \times n$ matrices over $D$, such that $\Phi(d)$ is the scalar matrix $dI_n$ whenever $d \in D$. A *symmetric representation* of $\Delta$ over $D$ is a representation of $\Delta$ over $D$ such that $\Phi(\delta)$ is symmetric whenever $\delta \in \Delta$. (This differs from the usual definition of a representation.)

Whenever $p(x) \in D[x]$ we have $\Phi(p(\delta)) = p(\Phi(\delta))$ for all $\delta \in \Delta$. Consequently, we may *assume that $\Delta$ is integrally dependent on $D$.* When $\Delta = D[\theta]$ the study of representations corresponds to the study of the matrices in $D_n$ which have $\theta$ as a characteristic root [10]. A unique extension of $\Phi$ to a representation of $G$ over $F$ exists and is determined by $\Phi(\theta)$.

DEFINITION. If $\Phi$ and $\Psi$ are representations of $\Delta$ over $D$ such that

$$(*) \qquad T\Phi(\delta)T^{-1} = \Psi(\delta) \qquad \text{for all } \delta \in \Delta$$

and some nonsingular $T \in D_n$ satisfying $T^{-1} \in D_n$, then $\Phi$ is *equivalent to* $\Psi$. The equivalence class of $\Phi$ is written $\mathcal{C}(\Phi)$.

Received December 19, 1966.

[1] I would like to thank my thesis advisor Dr. Taussky for her aid on my thesis [1] of which this is part. My thesis research was supported by a National Science Foundation Cooperative Graduate Fellowship.

[2] The case in which one also requires that $p(x)$ be quadratic has been discussed extensively [1], [11]–[13]. A revised presentation of the contents of [1] is planned.

Since $\Phi(\theta)$ determines $\Phi$, one may speak of a class of matrices $\mathcal{C}(\Phi(\theta))$ rather than a class of representations. Then $(*)$ is equivalent to

$$T\Phi(\theta)T^{-1} = \Psi(\theta).$$

Note that $T, T^{-1} \epsilon D_n$ is equivalent to $T$ being unimodular over $D_n$.

When $D = F$, there is exactly one equivalence class. This is a special case of Theorem 1 below.

## 3. Earlier results

We now give generalizations of some results which have been proved for the special case $D = \mathbf{Z}$.

THEOREM 1. *There is a one-to-one correspondence between classes of representations of $\Delta$ over $D$ and classes of ideals in $\Delta$ having a free basis over $D$.*

The proof is an easy generalization of that given by Taussky [10]. Let $\bar{\alpha}$ be a characteristic vector of $\Phi(\theta)$ with components in $G$. We have

$$\mathcal{C}(\Phi) \leftrightarrow \mathcal{C}(D\alpha_1 + \cdots + D\alpha_n = \mathfrak{a}).$$

It is convenient to *identify* $\mathcal{C}(\Phi)$ *with* $\mathcal{C}(\mathfrak{a})$. When $D = \mathbf{Z}$ or $D = F$, every ideal has a free basis.

Let $A'$ be the transpose of $A \epsilon D_n$ and define $\Phi'$ by $\Phi'(\delta) = \Phi(\delta)'$. Let $\mathfrak{a}'$ be the complement [7, p. 41] of $\mathfrak{a}$. By the method of proof used by Taussky [13] we have

THEOREM 2. *If* $\mathcal{C}(\Phi) \leftrightarrow \mathcal{C}(\mathfrak{a})$, *then* $\mathcal{C}(\Phi') \leftrightarrow \mathcal{C}(\mathfrak{a}')$.

It is known [11] that $\mathcal{C}(\Phi) = \mathcal{C}(\Phi')$ is not enough to guarantee a symmetric $\Psi \epsilon \mathcal{C}(\Phi)$. Various additional conditions are found in the literature. Some are given below.

THEOREM 3. *Let* $\mathfrak{a}$ *be in* $\mathcal{C}(\Phi)$. *The following are equivalent.*

(1) $\mathcal{C}(\Phi)$ *contains a symmetric representation.*

(2) *For every (or some)* $\Psi \epsilon \mathcal{C}(\Phi)$, *there is a matrix $T$ unimodular over $D_n$ such that*

$$T'T\Psi(\theta) = \Psi'(\theta)T'T \qquad \text{[11, Theorem 2].}$$

(3) *For some* $\lambda \epsilon G$ *and some free basis* $\bar{\alpha}$ *for* $\mathfrak{a}$ *over* $D$

$$\operatorname{tr}_{G/F} \lambda\alpha_i \alpha_j = \delta_{ij} \qquad \text{(Kronecker } \delta\text{) [4].}$$

*The following are consequences of* (1).

(a) *If $F$ is formally real, $G$ is totally real* [6, Theorem 3.3].

(b) *For some totally positive* $\lambda \epsilon G$ *we have* $\mathfrak{a}' = \lambda\mathfrak{a}$. (*"Totally positive" is a vacuous condition if $F$ is not formally real.*) *See* [4].

(c) *For* $\lambda$ *as in* (b) *and some* $f \in F$

$$N_{G/F}\lambda = (-1)^{n(n-1)/2} f^2 N_{G/F}\, p'(\theta)$$

*where* $p(x)$ *is the irreducible monic polynomial for* $\theta$ *over* $F$.

*Proof.* Where a reference is given, that proof is easily generalized to yield the desired result. Let $\bar{\beta}$ be the complementary basis to $\bar{\alpha}$. By (3) we have $\bar{\beta} = \lambda\bar{\alpha}$ (incidentally proving (b)). Thus

$$((\lambda^{(i)}\delta_{ij})) = ((\beta_j^{(i)}))((\beta_i^{(j)}))$$

where superscripts denote conjugacy. Taking determinants and noting that

$$\bar{\beta} = T(1, \theta, \cdots, \theta^{n-1})'$$

for some $T \in F_n$, we obtain (c). ▌

Parts (a)–(c) of the above theorem provide conditions of a more algebraic number theoretic nature than do (1)–(3). Unfortunately, it is not known when conditions (a)–(c) for an ideal with a free basis over $D$ imply the existence of a symmetric representation in $\mathfrak{C}(\mathfrak{a})$. When $n$ is odd and $D$ is an algebraic number field, then (a) implies (1) [2]. When $n \leq 7$ and $D = \mathbf{Z}$, then (a) and (b) imply (1) ([4], or Section 5 below). If (a)–(c) are satisfied for an ideal $\mathfrak{a}$ with a free basis $\bar{\alpha}$ over $D$, then define

$$S = ((\mathrm{tr}_{G/F}\,\lambda\alpha_i\,\alpha_j)).$$

It follows that $S$ is symmetric and

(i) unimodular over $D_n$ by (b),
(ii) positive definite if $F$ is formally real by (a) and (b),
(iii) of square determinant by (c).

By Theorem 3(3), it follows that $\mathfrak{C}(\mathfrak{a})$ contains a symmetric representation if and only if $S = X'X$ for some $X$ unimodular over $D_n$.

COROLLARY. *Every finite field of odd characteristic has a symmetric representation over each of its subfields.*

*Proof.* Since the norm group of $G$ over $F$ is the multiplicative group of $F$, there is a $\lambda \in D$ satisfying Theorem 3(c).

A nonsingular quadratic form ($S$ of the above discussion) has its dimension and its determinant as a complete set of invariants [9, 62:1a]. The corollary follows from the discussion preceding it. ▌

## 4. Number of symmetric representations

In this section we discuss the number of symmetric representations in a class and, briefly, the number of classes containing symmetric representations. When limiting attention to one class the relevant domain is not $\Delta$ but one we now define.

DEFINITION. $R(\Phi) = \{\alpha \mid \alpha \in G \text{ and } \Phi(\alpha) \in D_n\}$ where $\Phi$ has been extended to a representation of $G$ over $F$.

Clearly $R(\Phi)$ is an integral domain between $G$ and $\Delta$. If $\Psi \in \mathcal{C}(\Phi)$, then $R(\Psi) = R(\Phi)$; so $R(\Phi)$ is a class invariant. (In terms of the generalized ideal quotient we have $R(\Phi) = (\mathfrak{a} : \mathfrak{a})$.)

THEOREM 4. *Let $\Phi$ be a symmetric representation of $\Delta$ over $D$. The number of symmetric representations in $\mathcal{C}(\Phi)$ is a multiple of $k$ and is bounded above by*

$$k[U^N : U^2]$$

*where*

(1) $\mathcal{O}(D_n) = \{X \in D_n \mid X'X = I\}$,

(2) $k = \text{card } \mathcal{O}(D_n)$ *if $F$ has characteristic* 2
$= \frac{1}{2} \text{card } \mathcal{O}(D_n)$ *otherwise,*

(3) $U^2$ *is the group of squares of units in* $R(\Phi)$,

(4) $U^N$ *is the group of totally positive units in $R(\Phi)$ whose norms are squares in $D$.*

*Proof.* We shall use the well known fact that if $A, B \in F_n$ and $A$ has distinct roots and $AB = BA$, then $B = p(A)$ for some $p(x) \in F[x]$.

Let $A = \Phi(\theta)$. If $\Psi \in \mathcal{C}(\Phi)$, then $\Psi(\theta) = TAT^{-1}$ for some $T$ unimodular over $D_n$. Since $A = A'$, we have $\Psi = \Psi'$ if and only if $T'T = p(A)$ for some $p(x) \in F[x]$. For each $\eta \in G$ let $\varphi(\eta)$ be the set of $T$ unimodular over $D_n$ satisfying $T'T = \Phi(\eta)$. Clearly $\varphi(\eta) \neq \emptyset$ implies $\eta \in U^N$. The converse is equivalent to achieving the bound given by the theorem. It will be discussed after the proof.

If $T \in \varphi(\eta)$, then

$$\varphi(\eta) = \{XT \mid X \in \mathcal{O}(D_n)\}.$$

Hence $\text{card } \varphi(\eta) = \text{card } \mathcal{O}(D_n)$ whenever $\varphi(\eta) \neq \emptyset$.

All that remains is to study the equation

$$TAT^{-1} = SAS^{-1}, \qquad S, T \text{ unimodular over } D_n.$$

This is equivalent to $S^{-1}T = q(A)$ for some $q(x) \in F[x]$. Unimodularity of $S^{-1}T$ is equivalent to $q(\theta) = \varepsilon$ being a unit in $R(\Phi)$. We have

$$T'T = q(A)S'Sq(A)$$

so $T \in \varphi(\eta)$ if and only if $S \in \varphi(\eta\varepsilon^2)$. If $\eta = \eta\varepsilon^2$, then $\varepsilon = \pm 1$ so every nonempty $\varphi(\eta)$ leads to $k$ symmetric representations. Any two $\varphi(\eta)$ and $\varphi(\nu)$ lead either to the same (if $\eta/\nu \in U^2$) or to distinct (if $\eta/\nu \notin U^2$) representations. ▌

The bound in the theorem will be achieved if $\eta \in U^N$ implies $\varphi(\eta) \neq \emptyset$. By the definition of $U^N$ we see that $\Phi(\eta)$ is symmetric and

(i) unimodular over $D_n$,
(ii) positive definite if $F$ is formally real,
(iii) of square determinant.

We have $\varphi(\eta) \neq \emptyset$ if and only if $T'T = \Phi(\eta)$ for some $T$ unimodular over $D_n$. This is precisely the same problem as in Section 3(i)–(iii).

We now consider the number of classes containing symmetric representations when *all ideals are invertible.* Suppose $\mathfrak{C}(\mathfrak{a})$ contains a symmetric representation. The map $\mathfrak{C}(\mathfrak{b}) \leftrightarrow \mathfrak{C}(\mathfrak{a}\mathfrak{b})$ is a correspondence between classes containing ideals whose squares are narrowly equivalent to $\Delta$ and classes containing ideals narrowly equivalent to their complements (since $(\mathfrak{a}\mathfrak{b})' = \mathfrak{a}'\mathfrak{b}^{-1}$). Hence the number of classes containing symmetric representations is bounded by the order of the maximal subgroup of type $(2, 2, \cdots)$ in the ideal class group.

## 5. The rational integer case

For the remainder of the paper we will assume that $D = \mathbf{Z}$. This case has been studied by Faddeev [4] and Taussky [10]–[13]. In Theorem 4 we have $k = n!\,2^{n-1}$ since $\mathfrak{O}(\mathbf{Z}_n)$ consists of those matrices having one $\pm 1$ in each row and column and zeros elsewhere. By the Dirichlet unit theorem $[U^N : U^2]$ divides $2^{n-1}$. Since the class number of $\Delta$ is finite [3] we have

THEOREM 5. *The number of symmetric representations of $\Delta$ over $\mathbf{Z}$ is finite.*

Of particular interest are conditions (i)–(iii) of Sections 3 and 4. When $n \leq 7$ these conditions imply that the quadratic form is equivalent to a sum of squares [9, 106:10]. When $D = \mathbf{Z}$, (b) of Theorem 3 implies (c) because $T\bar{\beta} = \lambda\bar{\alpha}$ where $\det T = +1$. Hence

THEOREM 6. *Assume $n \leq 7$ and $G$ is totally real. There exists a symmetric representation of $\Delta$ over $\mathbf{Z}$ if and only if $\mathfrak{a}' = \lambda\mathfrak{a}$ for some ideal $\mathfrak{a}$ of $G$ and some totally positive $\lambda \in G$. In this case $\mathfrak{C}(\mathfrak{a})$ contains precisely $n!\,2^{n-1}[U^N : U^2]$ symmetric representation where $U^N$ and $U^2$ are as in Theorem 4.*

If we further assume that $\Delta$ is integrally closed in $G$ over $\mathbf{Z}$, then the existence of a symmetric representation is equivalent to the different being narrowly equivalent to the square of an ideal. It is known [5, Theorem 176] that the class of the different has a square root; but it is not known when this is true in the narrow sense. Faddeev [4] has used this result to establish the existence of symmetric representations for special $G$'s. Other special cases can be dealt with.

COROLLARY. *If $G$ is a cyclic cubic extension of $\mathbf{Q}$, the integers of $G$ have a symmetric representation over $\mathbf{Z}$.*

*Proof.* Let $p$ be a rational prime. It has at most one ramified divisor $\mathfrak{p}$ over $G$, and this is pure ramified. Thus, if the discriminant is $\Pi p^{c(p)}$, then the different is $\Pi \mathfrak{p}^{c(p)}$. Since $G$ is cyclic, every $c(p)$ is even.

## References


1. E. Bender, *Symmetric representations of an integral domain over a subdomain*, doctoral thesis, California Institute of Technology, 1966.
2. ———, *Characteristic polynomials of symmetric matrices*, to appear.
3. R. Dedekind, *Gesammelte mathematische Werke I*, Friedr. Vieweg u. Sohn, Braunschweig, 1930, pp. 105–157.
4. D. K. Faddeev, *On the characteristic equations of rational symmetric matrices*, (Russian)Dokl. Akad. Nauk SSSR, vol. 58 (1947), pp. 753–754.
5. E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Akad. Verlagsgesellschaft, Leipzig, 1923.
6. F. Krakowski, *Eigenwerte und Minimalpolynome symmetrischer Matrizen in kommutativen Körpern*, Comm. Math. Helv., vol. 32 (1958), pp. 224–240.
7. S. Lang, *Algebraic numbers*, Addison-Wesley, Reading, Mass., 1964.
8. C. Latimer and C. MacDuffee, *A correspondence between classes of ideals and classes of matrices*, Ann. of Math., vol. 34 (1933), pp. 313–316.
9. O. T. O'Meara, *Introduction to qudratic forms*, Grund. Math. Wiss., vol. 117, Academic Press, New York, 1963.
10. O. Taussky, *On a theorem of Latimer and MacDuffee*, Canad. J. Math., vol. 1 (1949), pp. 300–302.
11. ———, *Classes of matrices and quadratic fields*, Pacific J. Math., vol. 1 (1951), pp. 127–132.
12. ———, *Classes of matrices and quadratic fields II*, J. Lond. Math. Soc., vol. 27 (1952), pp. 237–239.
13. ———, *On matrix classes corresponding to an ideal and its inverse*, Illinois J. Math., vol. 1 (1957), pp. 108–113.


Harvard University
Cambridge, Massachusetts