MATRIX CLASSES AND IDEAL CLASSES

BY

ALPHONSE BUCCINO[1]

1. Introduction

Let R be an integral domain, K its quotient field, $f(X)$ a monic polynomial of degree n over R, $S = R[X]/f(X)R[X]$, and $L = K[X]/f(X)K[X]$; denote by x the canonical image of X in L. A one-to-one correspondence between similarity classes of cyclic matrices over R with the same characteristic polynomial $f(X)$ and classes of ideals of S which are free R-modules of rank n has been studied in [3] where $R = Z$ (the rational integers), and $f(X)$ has distinct irreducible factor with non-zero constant term; and in [4] where $R = Z$ and $f(X)$ is irreducible. In [5] with $R = Z, f(X)$ irreducible and S the ring of integers in the algebraic number field L it is shown that if an ideal I is in the class corresponding to a matrix A then I^{-1} is in the class corresponding to A', the transpose of A. This was done by making use of the complementary ideal [2, p. 41]. In [1] it is shown that the methods of [5] extend to cyclic matrices over any integral domain R with characteristic polynomial irreducible and separable over K. The conclusion there is that the transpose of a matrix corresponds to the complement of the ideal corresponding to the given matrix.

We show here that the correspondence in question always exists for cyclic matrices over any integral domain with no conditions on the characteristic polynomial and that the transpose matrix always corresponds to the inverse ideal. We do this by showing that the expression of the ideal class corresponding to the transpose matrix in terms of the ideal class corresponding to the given matrix arises by dualizing with respect to a non-degenerate associative bilinear form on L over K. We then show that there always exists such a bilinear form with respect to which the dual of an ideal is its inverse.

2. The correspondence

Two $n \times n$ matrices A and B over R are called *similar over* R if $B = PAP^{-1}$ for some matrix P over R such that P^{-1} also has entries in R. A matrix A over R is called *cyclic* if its minimal and characteristic polynomials (as a matrix over K) coincide. By an *ideal of* S is meant an S-submodule of L; an *e-ideal* of S is an ideal which is a free R-module of rank n. The following lemma is well known.

Received June 22, 1967.

[1] I would like to thank Professor Irving Kaplansky for his help on my dissertation of which this is part. This work was done while I held a National Science Foundation Science Faculty Fellowship at the University of Chicago.

Lemma 1. *If I and J are two regular ideals of S (i.e. ideals containing non-divisors of zero), they are isomorphic S-modules if and only if $J = bI$ for some non-divisor of zero b in L.*

An ideal class is an equivalence class of the relation S-module isomorphism on the ideals of S.

Suppose A is an $n \times n$ cyclic matrix over R with characteristic polynomial $f(X)$. Thinking of A as acting on the R-module of n-tuples $V = R + \cdots + R$ (n copies), we make V into an S-module, which we denote for clarity by V_A, by defining $g(x)v = g(A)(v)$ for $g(x) \in S$ and $v \in V$. The next lemma is also well known.

Lemma 2. *If A and B are cyclic matrices over R with the same characteristic polynomial $f(X)$, then V_A and V_B are isomorphic S-modules if and only if A and B are similar over R.*

Theorem 1. *There is a one-to-one correspondence between similarity classes of cyclic matrices over R with the same characteristic polynomial $f(X)$ and classes of e-ideals of S.*

Proof. Let A be a cyclic matrix over R with characteristic polynomial $f(X)$. Embed V in $KV = K \oplus \cdots \oplus K$ (n copies), which is a vector space over K. As a matrix over K, A acts on KV and so, as above, the latter becomes an L-module, $(KV)_A$. Since A is cyclic, there is a w in $(KV)_A$ such that for any v in $(KV)_A$ there is g in L such that $v = gw$. For w with this property, let

$$I_w = \{g \text{ in } L \mid gw \text{ is in } V\}.$$

Clearly, I_w is an e-deal and the mapping $g \to gw$ is an S-module isomorphism of I_w onto V_A. In view of the two preceding lemmas, we now have a well-defined mapping of similarity classes of matrices to classes of e-ideals which is one-to-one. That every e-ideal class arises in this way is seen as follows. If I is an e-ideal of S with R-basis $g_1, \cdots, g_n$, let $A = (a_{ij})$ be the matrix defined by

$$xg_i = \textstyle\sum_j a_{ij}\, g_j. \tag{1}$$

By this definition, the action of A on V is determined by multiplication by x in I. Thus, the powers of A and of x satisfy the same linear relations over K. Thus A is cyclic with characteristic polynomial $f(X)$, and V_A must be S-module isomorphic to I. This completes the proof of the theorem.

3. The ideal class corresponding to the transpose matrix

Continuing with the same notation, for $I \subset L$ denote by I^{-1} the set of all b in L such that $bI \subset S$. Obviously, when I is a regular ideal of S, so is I^{-1}. It is well known that when I is regular, I^{-1} and $\mathrm{Hom}_S\ (I, S)$ are isomorphic S-modules. This fact provides a compelling reason to expect the result of Theorem 3, below.

A bilinear form σ_1 on L over K is called *non-degenerate* if for each $g \neq 0$ in L, there is $h \in L$ such that $\sigma_1(g, h) \neq 0$. We call σ_1 *associative if* $\sigma_1(g, hk) = \sigma_1(gk, h)$ for all $g, h, k \in L$. A linear functional σ on L over K induces an associative bilinear form σ_1 by setting $\sigma_1(g, h) = \sigma(gh)$. One can verify that every associative bilinear form on L over K arises in this way. If σ_1 is a bilinear form on L over K and $I \subset L$, define

$$I' = \{h \in L \mid \sigma_1(g, h) \in R \text{ for all } g \in I\};$$

call I' the *dual of I with respect of* σ_1.

THEOREM 2. *If σ_1 is a non-degenerate associative bilinear form on L over K and if an e-ideal I is in the class corresponding to the similarity class of a matrix A, then I' is an e-ideal in the class corresponding to the similarity class of a matrix A'.*

Proof. Suppose I is an e-ideal of S with R-basis $g_1, \cdots, g_n$. Then there exist unique $g_1', \cdots, g_n'$ $_n$such that $\sigma_1(g_i, g_j') = \delta_{ij}$. It is easily verified that I' is an e-ideal with R-basis $g_1', \cdots, g_n'$. Supposing $A = (a_{ij})$, we can assume (see the proof of Theorem 1)

$$xg_i = \sum_j a_{ij} g_j.$$

On the other hand, since I' is an e-ideal,

$$xg_j' = \sum_k r_{jk} g_k'$$

for some choice of the r_{jk} in K. Now, $\sigma_1(xg_i, g_j') = a_{ij}$, while $\sigma_1(g_i, xg_j') = r_{ji}$. The associativity of σ_1 means that $\sigma_1(xg_i, g_j') = \sigma_1(g_i, xg_j')$, from which it follows that $r_{jk} = a_{kj}$. This implies that $V_{A'}$ and I' are isomorphic S-modules from which the theorem follows.

If the polynomial $f(X)$ is irreducible and is separable over K, then the associative bilinear form induced by the trace in non-degenerate. In this case I' coincides with the complement of I to yield the results of [1] and [5].

The next definition introduces a linear functional on L over K such that, as promised in the introduction, the induced associative bilinear form is non-degenerate and with respect to which the dual of an ideal is its inverse.

DEFINITION. *For* $b \in L$ such that $b = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}$, with $b_i \in K$, define $\sigma(b) = b_{n-1}$.

LEMMA 4. *The function $\sigma : L \to K$ defined above is a linear functional on L and the induced associative bilinear form σ_1 is non-degenerate. Moreover, if I is an ideal of S, dualizing with respect to this, σ_1 yields $I' = I^{-1}$.*

Proof. The first part of the lemma is easily established. For the second part, it is clear that $I^{-1} \subset I'$. Now let $b \in I'$, $g \in I$ so that if

$$bg = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$$

we have $c_{n-1} \epsilon R$. Let

$$f(X) = a_0 + a_1 X + \cdots + a_{n-1} + X^n$$

so that

$$xbg = -c_{n-1} a_0 + (c_0 - c_{n-1} a_1)x + \cdots + (c_{n-2} - c_{n-1} a_{n-1})x^{n-1}.$$

Then, since $xb \epsilon I'$, we have $c_{n-2} - a_{n-1} c_{n-1} \epsilon R$. From the fact that a_{n-1} and c_{n-1} are in R, it follows that $c_{n-2} \epsilon R$. Continuing in this way, it is seen that $c_i \epsilon R$ for $i = 0, 1, \cdots, n - 1$ so that $b \epsilon I^{-1}$, which proves the lemma.

We can summarize the results up to this point as follows.

THEOREM 3. *There is a one-to-one correspondence between similarity of cyclic $n \times n$ matrices over an integral domain R with the same characteristic polynomial $f(X)$ and classes of ideals of $S = R[X]/f(X)R[X]$ which are free R-modules of rank n. Moreover, for the correspondence described above, if I is an ideal in the class of a matrix A then I^{-1} is in the class corresponding to the similarity class of A', the transpose of A.*

Note that when the complement of an ideal of S can be defined, it is in the same class as the inverse of the ideal.

REFERENCES

1. E. BENDER, *Classes of matrices over an integral domain*, Illinois J. Math., vol. 11 (1967), pp. 697–702.
2. S. LANG, *Algebraic numbers*, Addison-Wesley, Reading, Mass., 1964.
3. C. LATIMER AND C. MACDUFFEE, *A correspondence between classes of ideals and classes of matrices*, Ann. of Math. (2), vol. 34 (1933), pp. 313–316.
4. O. TAUSSKY, *On a theorem of Latimer and MacDuffee*, Canad. J. Math., vol. 1 (1949), pp. 300–302.
5. ———, *On matrix classes corresponding to an ideal and its inverse*, Illinois J. Math., vol. 1 (1957), pp. 108–113.

DEPAUL UNIVERSITY
CHICAGO, ILLINOIS