Similarity of Matrices Over Artinian Principal Ideal Rings

B. R. McDonald

Department of Mathematics
The University of Oklahoma
Norman, Oklahoma 73019

Submitted by Olga Taussky Todd

ABSTRACT

This paper discusses the theory of similarity of matrices over a commutative Artinian principal ideal ring R. It is shown that for the class matrices A such that $R[A]$ is R-free a "rational" canonical form is available.

I. INTRODUCTION

Let R denote a commutative Artinian principal ideal ring, $(R)_n$ denote the $n \times n$ matrix ring over R, and $\mathrm{GL}_n(R)$ denote the invertible matrices in $(R)_n$. It is well known that R decomposes uniquely as $R = R_1 \oplus \cdots \oplus R_m$, where R_i is a local Artinian principal ideal ring for $1 \leqslant i \leqslant m$. This decomposition induces a direct sum [product] decomposition of $(R)_n$ [$\mathrm{GL}_n(R)$]. Further, for this decomposition it is easy to see that if $A = A_1 \oplus \cdots \oplus A_m$ and $B = B_1 \oplus \cdots \oplus B_m$, where A and B are in $(R)_n$ and A_i and B_i are in (R_i), then $PAP^{-1} = B$ if and only if $P_i A_i P_i^{-1} = B_i$, where $P = P_1 \oplus \cdots \oplus P_m$ with P in $\mathrm{GL}_n(R)$ and P_i in $\mathrm{GL}_n(R_i)$. That is, R is similar to B if and only if A_i is similar to B_i for $1 \leqslant i \leqslant m$.

In view of the above remarks, we will assume throughout this paper that R is a local Artinian principal ideal ring. Let $m = (\theta)$ denote the maximal ideal of R, and $k = R/m$ the residue field of R. Let μ denote the canonical ring morphism $R \to R/m = k$. Let β denote the nilpotency of m, i. e., the smallest positive integer v with $\theta^v = 0$.

 0024-3795/78/0021-0153$01.25

Local Artinian principal ideal rings occur in several common settings. The best-known examples are Z/Zp^n (p a prime) and $k[X]/(p^a)$ (p an irreducible polynomial over the field k). They occur as local residue class rings of the rings of algebraic integers in finite extensions of the rationals (even though these domains are not principal ideal domains). Recently they have arisen as the coordinating rings of Desarguesian Hjemslev planes.

Matrices over Artinian principal ideal rings (especially Z/Zm and $k[X]/(f)$ where k is a finite field) have been of increasing interest in combinatorics, algebraic coding theory and algebraic cryptography.

II. REGULAR LINEAR MAPS

Let F denote a free R-module of R-dimension n. Let $\rho: F \to F$ denote an R-linear endomorphism of F.

The canonical projection $\mu: R \to k = R/m$ induces naturally surjective morphisms: $R[X] \to k[X]$, $F \to F/mF$ and $\mathrm{End}_R(F) \to \mathrm{End}_k(F/mF)$ [equivalently, $(R)_n \to (k)_n$]. Further, since R is local, the induced morphism $\mathrm{GL}_n(R) \to \mathrm{GL}_n(k)$ is surjective. A discussion of R-spaces (e.g., free R-modules) and their linear algebra is available in [5]. Each of these morphisms will also be denoted by μ. To illustrate the above, consider ρ in $\mathrm{End}_R(F)$. Then $\rho \to \mu\rho$, where $\mu\rho: F/mF \to F/mF$ by $(\mu\rho)(x+mF) = \rho(x) + mF = \mu(\rho(x))$. This is well defined, since $\rho(mF) \subseteq mF$. The corresponding matrix map $(R)_n \to (k)_n$ is given by $[a_{ij}] \to [\mu a_{ij}]$.

The following lemma is known for local rings (see [6], Theorems (5.1) and (5.3), pp. 13–14).

LEMMA II.1. *Let M be a finitely generated R-module. A subset $\{b_i\}$ is a minimal R-generating set for M if and only if its set of residue classes $\{\bar{b}_i\}$ form a k-basis for M/mM. Further, if $\{t_i | 1 \leqslant i \leqslant n\}$ and $\{c_j | 1 \leqslant j \leqslant \bar{n}\}$ are minimal generating sets for M, then $n = \bar{n}$ and there exists an invertible matrix P over R with $\langle b_1, \ldots, b_n \rangle P = \langle c_1, \ldots, c_n \rangle$.*

Since a free basis of F is a minimal generating set and $\mathrm{GL}_n(R)$ by the above is transitive on the set of minimal generating sets, the following lemma is clear.

LEMMA II.2. *A minimal generating set of a free R-module is free.*

We will use (II.2) in the next section.

Let $\rho: F \to F$ be an R-morphism. Let $\chi_\rho(X) = \det(X - \rho)$ denote the characteristic polynomial of ρ. Let $\lambda_\rho(X)$ denote the monic polynomial of least degree in $R[X]$ satisfying $\lambda_\rho(\rho) = 0$.

It is easy to see that $\chi_\rho(X)$ behaves favorably relative to the morphism μ, i.e., $\mu(\chi_\rho(X))=\chi_{\mu\rho}(X)$. However, in general, $\mu(\lambda_\rho(X))\neq\lambda_{\mu\rho}(X)$. We will see that it is precisely the fact that $\mu(\lambda_\rho(X))\neq\lambda_{\mu\rho}(X)$ that causes the difficulty with obtaining a canonical form under similarity. Observe that since $\lambda_\rho(\rho)=0$, we have $(\mu\lambda_\rho)(\mu\rho)=0$. Thus $\lambda_{\mu\rho}(X)$ divides $(\mu\lambda_\rho)(X)$. We call $\lambda_\rho(X)$ the *minimal polynomial of* ρ *in* $R[X]$.

To study a single endomorphism $\rho:F\to F$, it is well known that we actually study the ring $R[\rho]=\{\sum r_i\rho^i | r_i \text{ in } R\}$ generated by ρ in $\mathrm{End}_R(F)$ and the natural substitution morphism $R[X]\to R[\rho]$ given by $X\to\rho$. Let σ_ρ denote the substitution morphism $R[X]\to R[\rho]$. The kernel of σ_ρ is the *ideal of relations satisfied by* ρ.

We will call the endomorphism ρ *regular* if $R[\rho]$ is a free (non-zero) R-submodule of $\mathrm{End}_R(F)$.

Certainly $R[\rho]\cong R[X]/A$, where $A=\ker(\sigma_\rho)$ is the ideal of relations satisfied by ρ. Fortunately, Snapper [7–9] in the early 50s gave precise descriptions of ideals in $R[X]$ for R a local Artinian principal ideal ring. Suppose A is an ideal of $R[X]$, and suppose $\mu A\neq 0$. Since $k[X]$ has all its ideals principal, $\mu A=(\bar{f})$. Let f be a monic pre-image of $\bar{f}$ in A. Then A has the form $A=(f,N)$, where $N=A\cap(m[X])$, and where (f,N) denotes the ideal generated by f and N (see Sec. 12, pp. 691–692 of [7]). Further, since the maximal ideal $m=(\theta)$ is principal, the above description may be refined (see Secs. 8 and 9, pp. 57–60 of [9]). Precisely, let $A_i=\{g \text{ in } R[X] | \theta^i g \text{ is in } A\}$. One has a chain of ideals

$$A=A_0\subseteq A_1\subseteq\cdots\subseteq A_\beta=R[X]$$

($\beta=$ nilpotency of θ). If f_i denotes the monic polynomial of least degree in A_i, then $A_i=(f_i,N_i)$, where $N_i=A_i\cap m[X]$.

By [9] (pp. 58–59),

(a) $\deg(f_i)\leqslant\deg(f_{i-1})$,
(b) $A=(f_0,\theta f_1,\theta^2 f_2,\ldots,\theta^{\beta-1}f_{\beta-1})$, where $f_0=f$.

In particular, $R[X]/A$ is R-free if and only if $A=(f)$. The next result is now straightforward.

THEOREM II.3. *The R-morphism $\rho:F\to F$ is regular if and only if the kernel of the substitution morphism is a principal ideal generated by a monic polynomial.*

We next compare the minimal polynomials of ρ and $\mu\rho$ for a regular morphism.

Let ρ be an R-morphism and $A=\ker(\sigma_\rho)$. By the above discussion

$$A=(f_0,\theta^1 f_1,\ldots,\theta^{\beta-1}f_{\beta-1}).$$

Since $\theta^i f_i(\rho)=0$ for $1\leqslant i\leqslant \beta-1$, we have $f_i(\rho)=\theta^{s_i}g_i(\rho)$, where g_i is in $R[X]$ and $s_i=\beta-i$. Hence $f_i(\rho)$ is in the Jacobson radical,

$$\mathrm{Rad}(\mathrm{End}_R(F))\cong\{[a_{ij}]\,|\,a_{ij}\text{ is in }(\theta)=m\},$$

of $\mathrm{End}_R(F)$. Thus, $\mu(f_i(\rho))=0$, i.e., $(\mu f_i)(\mu\rho)=0$. Thus, μf_i is in the ideal of relations satisfied by $\mu\rho$, i.e., the principal ideal generated by the minimal polynomial $\lambda_{\mu\rho}$. By (a) above,

$$\deg(\lambda_{\mu\rho})\leqslant\deg(\mu f_{\beta-1})\leqslant\cdots\leqslant\deg(\mu f_1),$$

since each f_i is monic, and $\lambda_{\mu\rho}$ divides μf_i.

Observe that $\lambda_\rho=f(=f_0)$, and $\lambda_{\mu\rho}$ divides $\mu\lambda_\rho$. Suppose $\lambda_{\mu\rho}\neq\mu(\lambda_\rho)$. Select g, a monic polynomial in $R[X]$ with $\mu g=\lambda_{\mu\rho}$. Since $\mu(g(\rho))=\mu g(\mu\rho)=\lambda_{\mu\rho}(\mu\rho)=0$, $g(\rho)$ is in $\ker(\mu)=\mathrm{Rad}(\mathrm{End}_R(F))$. Hence $g(\rho)=\theta^t\bar{g}(\rho)$, where $\bar{g}$ is in $R[X]$ and $\bar{g}(\rho)$ has no factor θ. Then g is in $A_{\beta-t}=\{h\,|\,\theta^{\beta-t}h\text{ is in }A\}$. Thus, $A_{\beta-t}\neq 0$, i.e., A is not a principal ideal and ρ is not regular. This characterizes regular elements.

THEOREM II.4. *The R-morphism $\rho:F\to F$ is regular if and only if $\mu(\lambda_\rho)=\lambda_{\mu\rho}$.*

This theorem indicates that if the minimal polynomial λ_ρ of ρ maps to the minimal polynomial $\lambda_{\mu\rho}$ of $\mu\rho$, then ρ is regular and the similarity theory of the next section will apply.

It is not easy to compute λ_ρ. We now give a procedure based on some work of McCoy [4] in 1939.

The *first Fitting invariant*, denoted $F_1(A)$, of an $n\times n$ matrix A over a commutative ring, is the ideal generated by the determinants of all the $(n-1)\times(n-1)$ submatrices of A. Thus, $F_1(A)$ is precisely the ideal generated by the elements of $\mathrm{adj}(A)$—the adjoint of A. The invariant is independent of basis, i.e., $F_1(PAP^{-1})=F_1(A)$ for P in $\mathrm{GL}_n(R)$.

If M and N are two ideals in a commutative ring S, then the *quotient of M by N*, denoted (M,N), is

$$(M,N)=\{s\text{ in }S\,|\,sN\subseteq M\}.$$

Finally, recall that $\chi_\rho(X)$ denotes the characteristic polynomial of ρ. Then McCoy's theorem [4, Theorem 3], stated in the above terminology, is

$$\ker(\sigma_\rho) = \big((\chi_\rho) : F_1(X-\rho)\big),$$

i.e., the ideal of relations satisfied by ρ is the ideal quotient of the ideal generated by the characteristic polynomial χ_ρ and the first Fitting invariant of $X-\rho$. Since $F_1(X-\rho)$ is generated by the elements of $\operatorname{adj}(X-\rho)$, it is necessary to determine $\operatorname{adj}(X-\rho)$. Gantmacher [2, pp. 84–85] gives a formula over a field which will easily carry over to a commutative ring: If $\chi_\rho(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_n$, then $\operatorname{adj}(X-\rho) = X^{n-1} + \alpha_1 X^{n-2} + \cdots + \alpha_{n-1}$, where

$$\begin{aligned}
\alpha_1 &= \rho - a_{n-1}I,\\
\alpha_2 &= \rho^2 - a_{n-1}\rho - a_{n-2}I,\\
&\vdots\\
\alpha_{n-1} &= \rho^{n-1} - a_{n-1}\rho^{n-2} - \cdots - a_1 I.
\end{aligned}$$

III. THE CANONICAL MATRIX

We begin this section by summarizing some results on polynomial theory in $R[X]$.

A polynomial f in $R[X]$ is *regular* if $\mu f \neq 0$.

THEOREM III.1. *If f is a monic regular polynomial in $R[X]$, then f may be factored uniquely (up to order of factors) as*

$$f = g_1 \cdots g_s,$$

where the g_i are monic primary coprime polynomials.

Proof. This result is Theorem 5.1 of [7] with the addition that f and g_i are chosen to be monic to assure uniqueness. ∎

Let $\rho : F \to F$ be regular. Suppose $f = \lambda_\rho$, the minimal polynomial of ρ. Then f is a regular polynomial, and by Theorem III.1 $f = g_1 \cdots g_s$. Since g_i and g_j $(i \neq j)$ are coprime, $(f) = (g_1) \cdots (g_s) = \cap_i (g_i)$. Define

$$\pi : R[X] \to \oplus \sum_{i=1}^{s} R[X]/(g_i)$$

by

$$\pi : h \to \langle h + (g_1), \ldots, h + (g_s) \rangle.$$

This is surjective, and the kernel is $\ker(\pi) = (f) = \cap_i (g_i)$. (See Proposition 1.10, p. 7, [1].) That is, $R[X]/(f) \cong \oplus \Sigma_{i=1}^{s} R[X]/(g_i)$. Let $S = R[X]/(f)$ and $S_i = R[X]/(g_i)$, $1 \leqslant i \leqslant s$. Since g_i is primary, S_i is a local ring. Further, if e_i denotes the identity of S_i, then $1 = e_1 + \cdots + e_s$ gives a decomposition of the identity of S as a sum of orthogonal idempotents.

The R-space F is naturally an S-module via the action of ρ, i.e., if $h = \Sigma r_i X^i$ is in S and b in F, then

$$h \cdot b = (h(\rho))(b) = (\Sigma r_i \rho^i)(b).$$

The above decomposition of S induces a primary decomposition of F,

$$F = F_1 \oplus \cdots \oplus F_s,$$

where $F_i = e_i F$. This is also a splitting of F as an R-module. Since F is R-free, each F_i is a projective R-module. But (recall) projective modules over local rings are free. Hence, each F_i is R-free. Finally, the Krull-Schmidt theorem provides the uniqueness of the above decomposition.

The action on F_i of S is precisely the action on F_i of S_i. Hence, the above discussion allows us to restrict our attention to F_i which is acted on by $S_i = R[x]/(g_i)$ where g_i is a monic primary polynomial.

Thus, we now assume that f is a primary polynomial—i.e., (f) is a primary ideal—and return to the original context and notation.

Let $S = R[X]/(f)$ act on F through ρ. Since S is Artinian and F is a finitely generated S-module, F decomposes into a direct sum of indecomposable S-modules, say $F = E_1 \oplus \cdots \oplus E_w$. Again, the Krull-Schmidt theorem provides the uniqueness of such a decomposition.

Recall that if R were a field, then we would be done, since each E_i would be a cyclic S-module and the restriction of ρ to E_i would produce a companion matrix. It remains to show this is still the case in our extended situation.

The decomposition $F = E_1 \oplus \cdots \oplus E_w$ as an S-module $(S = R[X]/(f))$ is also a decomposition as an R-module. Thus, since F was R-free, the E_i are R-projective and hence free as R-modules.

We will examine one of the summands of F. Select i, $1 \leqslant i \leqslant w$, and let E_i be denoted by E. Then E is an indecomposable S-module and a free R-module. Modulo the maximal ideal m of R, E/mE is an $\bar{S} = k[X]/(\mu f)$-

module. Therefore, E/mE is a direct sum of cyclic $\bar{S}$-modules,

$$E/mE = \bar{S}\bar{b}_1 \oplus \cdots \oplus \bar{S}\bar{b}_r.$$

But $\bar{S} = k[X]/(\mu f) \cong k[\mu\rho]$. Thus, as a k-vector space,

$$E/mE = \left(\oplus \sum_{i=0}^{t_1} k\left[(\mu\rho)^i \bar{b}_1 \right] \right) \oplus \cdots \oplus \left(\oplus \sum_{i=0}^{t_r} k\left[(\mu\rho)^i \bar{b}_r \right] \right).$$

Letting b_i be a pre-image of $\bar{b}_i$, $1 \leqslant i \leqslant r$, we lift the basis back to a minimal R-generating set. That is, by Lemma II.1,

$$\{ b_1, \ldots, \rho^{t_1} b_1, \ldots, b_r, \ldots, \rho^{t_r} b_r \} \qquad (*)$$

is a minimal R-generating set for E. But E is R-free. Thus (*) is a free R-basis for E by Lemma II.2.

Also, it is clear that

$$E = Sb_1 + \cdots + Sb_r. \qquad (**)$$

Our aim is to show (**) is actually a direct sum; then, since E is assumed to be indecomposable, we must have $r = 1$ and $E = Sb_1$, i.e., E is a cyclic S-module.

In order to show this, we recall some facts on cyclic S-modules. Suppose Sb is a cyclic S-module, where b is R-free when Sb is considered as an R-module. It is well known that $Sb \cong S/A$ (as an S-module) where $A = \mathrm{Annih}_S(b)$ is an ideal of S. But the ideals of S are known. The ring $S = R[X]/(f)$, where f is primary. By [7] (Sec. 12), $f(X) = p(X)^\delta + n(X)$, where $p(X)$ is a fundamental irreducible, i.e., $p(X)$ remains irreducible modulo m, and $n(X)$ is in $m[X]$. Then [8] (p. 128, Statement 3.2) shows the maximal ideal of $R[\rho]$ is generated by θ and τ, where $m = (\theta)$ and $\tau = p(\rho)$. Since b is R-free, $\mathrm{Annih}_S(b) = S\tau^i = (\tau^i)$ for some i, $1 \leqslant i \leqslant \delta$.

Returning to (**), suppose

$$s_1 b_1 + \cdots + s_n b_n = 0 \qquad (***)$$

with s_i in S. Further,

$$s_i b_i = \left(\sum_j r_{ij} \rho^j \right) b_i$$

for some r_{ij} in R. If $\mathrm{Annih}_S(b_i) = (\tau^{\delta_i}) = \left(p(\rho)^{\delta_i} \right)$, then in $R[X]$

$$\sum_j r_{ij} X^j = p(X)^{\delta_i} h_i(X) + v_i(X),$$

where either the remainder $v_i(X)$ is 0 or $\deg(v_i(X)) < \delta_i \deg(p(X))$.

Suppose $v_i(X) = \sum_{k=1}^{z_i} a_{ik} X^k$ for a_{ik} in R. Then

$$\begin{aligned} 0 &= \sum_i s_i b_i \\ &= \sum_i \left(\sum_k a_{ik} \rho^k \right) b_i \\ &= \sum_{i,k} a_{ik} \left(\rho^k b_i \right). \end{aligned}$$

But the set (*) is R-free. Hence $a_{ik} = 0$ for all i and k. Thus $v_i(X) = 0$, and we conclude $s_i b_i = 0$ for $1 \leqslant i \leqslant t$ in (***). Thus the b_i are independent (see [3], pp. 390–391), and

$$E = Sb_1 \oplus \cdots \oplus Sb_r$$

as an S-module. Since E is S-indecomposable, this is not possible unless $r = 1$. We conclude that

$$E = Sb \qquad \text{(as an S-module)}$$

and

$$E = Rb \oplus R\rho b \oplus \cdots \oplus R\rho^{t-1} b \qquad \text{(as an } R\text{-module)},$$

where $t = \deg(f)$. Further, E is R-free. Thus, with respect to the R-basis

$\{b, \rho b, \ldots, \rho^{t-1}b\}$ of E, the matrix of ρ is

$$C(\rho) = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -a_{t-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{t-1} \end{bmatrix},$$

the *companion* matrix of $f(X) = \sum_{i=0}^{t} a_i X^i$.

Summarizing the discussion of this section, we have the following theorem.

THEOREM III.2. *Let R be a local Artinian principal ideal ring, F a free R-module of R-dimension n and $\rho: F \to F$ a regular R-morphism. Then a basis of F may be chosen such that relative to this basis*

$$\mathrm{Mat}(\rho) = \mathrm{diag}[T(g_1), \ldots, T(g_s)],$$

where $f = g_1 \cdots g_s$ generates the kernel of the substitution morphism $R[X] \to R[\rho]$, g_i is primary, and $T(g_i)$ is a diagonal sum of companion matrices

$$T(g_i) = \begin{bmatrix} C(p_i^{\delta_1}) & & & 0 \\ & C(p_i^{\delta_2}) & & \\ & & \ddots & \\ 0 & & & C(p_i^{\delta_t}) \end{bmatrix}.$$

The author is indebted to Joel Brawley for motivating this paper.

REFERENCES

1 M. F. Atiyah, and I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, Mass., 1969.
2 F. R. Gantmacher, *The Theory of Matrices*, Chelsea, New York, 1960.
3 S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1965.

4 N. H. McCoy, Concerning matrices with elements in a commutative ring, *Bull. AMS* **45** (1939), pp. 280–284.
5 B. R. McDonald, *Geometric Algebra over Local Rings*, Dekker, New York, 1976.
6 M. Nagata, *Local Rings*, Interscience, New York, 1962.
7 E. Snapper, Completely primary rings, I, *Ann. Math.* **52** (1950), pp. 666–693.
8 E. Snapper, Completely primary rings, II, *Ann. Math.* **53** (1951), pp. 125–142.
9 E. Snapper, Completely primary rings, IV, *Ann. Math.* **55** (1952), pp. 46–64.
10 O. Zariski and P. Samuel, *Commutative Algebra I*, Van Nostrand, New York, 1958.

Received November 1976; revised April 1977