A CANONICAL SET FOR MATRICES OVER A PRINCIPAL IDEAL RING MODULO m

L. E. FULLER

1. Introduction. If $m \in P$ where P is a p.i.r. (principal ideal ring), then $P/\{m\}$ is a commutative ring with unit element. The elements of this ring are designated by $\bar{a}$ where $a \in P$. The set of square matrices of order n with elements in $P/\{m\}$ forms a ring with unit element. The units in this ring are the unimodular matrices, i.e., the matrices whose determinants are units of $P/\{m\}$. By the following definition, these unimodular matrices determine equivalence classes in the ring of matrices.

Two matrices A and B are *row equivalent*, or *left associates*, if there exists a unimodular matrix U such that $UA = B$.

We shall derive a canonical set for our matrices under row equivalence. This was first done by the author for P the ring of integers **(1)**. The present paper simplifies and extends that result.

2. The canonical set. The basic case to be considered is for $m = p^k$, p a prime in P, and k a positive integer. An element $a \in P$ and p^k have a g.c.d. of the form p^t where $0 \leqslant t \leqslant k$. We designate $d(a) = t$ as the *degree* of the element a. All elements of the same degree are associates in $P/\{p^k\}$. If an element is of degree zero, it has an inverse in $P/\{p^k\}$ and hence is a unit. If $d(a) = k$, then the element is in the zero class in the modular ring. All other elements are proper divisors of zero in $P/\{p^k\}$. The elements $\bar{a}$ of $P/\{p^k\}$ thus belong to one of $k + 1$ ordered classes. The order of a class is determined by the degree of any element in it. For convenience, the bar over the elements of $P/\{p^k\}$ will be dropped when they are elements of a matrix.

THEOREM 1. *Every nth order matrix with elements in* $P/\{p^k\}$ *is the left associate of a matrix having the following properties*:

1. The degree of every element is at least equal to the degree of the diagonal element of its row, that is, $d(a_{rs}) \geqslant d(a_{rr})$ for all r and s.

2. The degree of every element above the diagonal is greater than the degree of the diagonal element of its row unless that diagonal element is zero, i.e., $d(a_{rs}) > d(a_{rr})$ for all $s > r$ if $a_{rr} \neq 0$.

3. Every diagonal element is of the form p^t, $0 \leqslant t \leqslant k$.

4. If for $r \neq s$, $d(a_{rs}) \geqslant d(a_{ss})$, then $a_{rs} = 0$. If $d(a_{ss}) > d(a_{rs})$, then $a_{rs} \in P/\{p^k\}/\{a_{ss}\}$, that is, a_{rs} is unique modulo a_{ss}.

Properties 1 and 2 give the relationship between the elements in a row and their diagonal element. Property 4 does this for the elements in a column and

Received July 27, 1953; in revised form May 31, 1954.

their diagonal element. Property 3 uses a convenient representative for the classes of elements of the same degree.

The second property could be applied to the elements below the diagonal instead of to those above. For uniqueness, it is necessary to have it one way or the other. For the exception noted in Property 2, $a_{rs} = 0$ for all s by Property 1. This would be true for either form of 2.

If $k = 1$, then $P/\{p^k\}$ is a field. The elements are either of degree 1 (if $= 0$) or of degree 0. By Property 3 all diagonal elements are either zero or unity. If the diagonal element is zero, the rest of the row is zero by 1. If the diagonal element is of degree 0, the rest of the column is zero by 4. By Property 2, the matrix is triangular with zeros above the diagonal. These properties are those of the Hermite form for a square matrix over a field.

Before proving the theorem, let us outline briefly how the diagonal elements are to be chosen. Each element of the matrix belongs to one of the $k + 1$ ordered classes based on their degrees. We consider those in the class of lowest degree for the given matrix. For the first diagonal element, we choose any one in this class with one exception. When a row contains more than one element of the class of lowest degree, our choice in property 2 requires that we consider only the element with the highest column index. In step 2 we form a submatrix by deleting the column used in step 1 and the corresponding row. From this subarray, a choice of a second element in made in exactly the same manner. At each succeeding step, one more column and the corresponding row are deleted. An element is then selected from the resulting square submatrix as in the first step.

Step 1. By an interchange of rows, if necessary, place the chosen element in the diagonal position. This element can then be changed to a power of p by using a suitable unit as a multiplier. Because of the way in which the diagonal element was selected, all other elements of the column are multiples of it. By elementary transformations these can be reduced to zero. The index of this column and the corresponding row will be designated as the $\bar{1}$st.

Step 2. Make a choice of a new element from the submatrix formed without the $\bar{1}$st row and column. Place this element in the diagonal position and change it to a power of p. The elements in this column will, as before, be multiples of this diagonal element so that they can be reduced to zero. The one possible exception to this is the element in the $\bar{1}$st row. It can be transformed to the representative of its residue class modulo this new diagonal element. The index of this column and the corresponding row will be designated as the $\bar{2}$nd.

In general, the $\bar{h}$th diagonal element is chosen from the submatrix formed by the deletion of the rows and columns designated as $\bar{j}$th for $j = 1, \ldots, h - 1$. The selected element is placed in the diagonal and transformed to a power of p. All elements in rows not designated as yet are multiples of this diagonal element and can be reduced to zero. The elements in designated rows belong to residue classes modulo this $\bar{h}$th diagonal element. Each can then be transformed to the representative of its class.

Working with elements of least degree ensures Property 1. The choice of the element with the higher column index gives us Property 2. Properties 3 and 4 obviously follow from what is done after the selection of a diagonal element.

3. Uniqueness of the canonical set. To prove uniqueness, we assume that two canonical matrices A and B are in the same row equivalence class. Under this assumption, there exists a unimodular matrix Q such that $QA = B$. We must prove that $A = B$. This is done by an induction on the columns of A and B in the matrix equation. For the induction, we shall order the columns of A first according to the degrees of their diagonal elements, starting with the columns whose diagonal elements are of least degree. Then for those of the same degree, we order according to their indices, starting with the largest one. The degrees of the diagonal elements thus form a non-decreasing sequence under the specified ordering. There is always an increase in the degree whenever the column index is increased. This ordering is similar to that used in choosing the diagonal elements, the only difference being in the final ordering of the indices. This is done to simplify the proof. Because of this similarity, the bar notation will again be used to designate the ordering. At each step the degrees of the elements involved in the equations will play a key role. The *reductio ad absurdum* proof will come from an equation with the left side having all terms of higher degree than the single term on the right side. This situation will arise as a consequence of certain combinations of Property 2 and the following lemma, where it is assumed $a_{\bar{h}\bar{h}} \neq 0$.

LEMMA 1. *If for* $i \geqslant h$:

(a) $\bar{h} \geqslant \bar{\imath}$, *then* $d(a_{\bar{\imath}\bar{\imath}}) \geqslant d(a_{\bar{h}\bar{h}})$,
(b) $\bar{h} < \bar{\imath}$, *then* $d(a_{\bar{\imath}\bar{\imath}}) > d(a_{\bar{h}\bar{h}})$.

This is the symbolic statement of the ordering on the columns of A that we are using.

LEMMA 2. *If* $i > h$, *then* $a_{\bar{\imath}\bar{h}} = 0$.

By Property 1 and Lemma 1, the following inequalities hold:

$$d(a_{\bar{\imath}\bar{h}}) \geqslant d(a_{\bar{\imath}\bar{\imath}}) \geqslant d(a_{\bar{h}\bar{h}}).$$

The conclusion is a consequence of Property 4.

Since Q is unimodular, it must have at least one unit in every row and column. We shall see that the only elements of degree zero will be the identity elements in the diagonal unless some diagonal element of A is zero. Then the corresponding column of Q will be arbitrary.

THEOREM 2. *The canonical set is unique.*

The $\bar{1}$st column of A contains all zeros except possibly the diagonal element, by Lemma 2. If it were also zero, then all diagonal elements of A would be zero by Lemma 1. Then by Property 1, A would be the zero matrix. It follows

that B must also be the zero matrix. In this event we have $A = B$ at once. In case the diagonal element is non-zero, the equations for this column take the simple form:

$$q_{\bar{r}\bar{1}}\, a_{\bar{1}\bar{1}} = b_{\bar{r}\bar{1}}, \qquad r = 1, \ldots, n.$$

Since Q is unimodular, some $q_{\bar{r}\bar{1}}$ must be of degree zero. If $d(q_{\bar{1}\bar{1}}) = 0$, then $d(a_{\bar{1}\bar{1}}) = d(b_{\bar{1}\bar{1}})$. By Property 3, $a_{\bar{1}\bar{1}} = b_{\bar{1}\bar{1}}$ so that $q_{\bar{1}\bar{1}}$ is the identity element. Consequently, $d(b_{\bar{r}\bar{1}}) \geqslant d(b_{\bar{1}\bar{1}})$ for all r. Therefore by Property 4, $b_{\bar{r}\bar{1}} = 0$ for $r \neq 1$. This means that $q_{\bar{r}\bar{1}}\, a_{\bar{1}\bar{1}} = \delta_{\bar{r}\bar{1}}\, a_{\bar{1}\bar{1}}$, so that only the $q_{\bar{1}\bar{1}}$ is a unit in the $\bar{1}$st column of Q. Because $d(a_{\bar{1}\bar{s}}) \geqslant d(a_{\bar{1}\bar{1}})$, $q_{\bar{r}\bar{1}}\, a_{\bar{1}\bar{s}} = \delta_{\bar{r}\bar{1}}\, a_{\bar{1}\bar{s}}$ for all s by Property 1.

If $q_{\bar{1}\bar{1}}$ were not a unit, then some other $q_{\bar{r}\bar{1}}$ would be of degree zero. We can derive a contradiction to this assumption by considering the equation involving the $\bar{r}$th diagonal of B:

$$\sum_{\bar{i}} q_{\bar{r}\bar{i}} a_{\bar{i}\bar{r}} = b_{\bar{r}\bar{r}}.$$

We know that

$$d(a_{\bar{i}\bar{r}}) \geqslant d(a_{\bar{r}\bar{i}}) \geqslant d(a_{\bar{1}\bar{1}}) = d(b_{\bar{r}\bar{1}}) \geqslant d(b_{\bar{r}\bar{r}}).$$

The first and last inequalities hold by Property 1. The strict equality is a result of the assumption on $q_{\bar{r}\bar{1}}$. The other inequality follows by Lemma 1. We shall now see that at least one of the three $\geqslant$'s is a strict inequality for each $\bar{i}$. This gives a false equation with all terms on the left of higher degree than the one on the right.

If $\bar{1} > \bar{r}$, the last inequality is a strict inequality by property 2 of the canonical set. If $\bar{r} > \bar{1}$ and $\bar{i} > \bar{1}$, the second $\geqslant$ is now strict by Lemma 1(b), since $i > 1$. If $\bar{r} > \bar{1}$ and $\bar{1} \geqslant \bar{i}$, then $\bar{r} > \bar{i}$ so that the first $\geqslant$ cannot be an equality, by Property 2.

Assume that the $\bar{j}$th column of A is the same as the corresponding column of B for $j = 1, \ldots, h-1$. We shall now show this to be true for the $\bar{h}$th column of A. From our assumption we know that for all $j < h$,

$$q_{\bar{r}\bar{j}}\, a_{\bar{j}\bar{s}} = \delta_{\bar{r}\bar{j}}\, a_{\bar{j}\bar{s}}.$$

By Lemma 2, we also known that $a_{\bar{r}\bar{h}} = 0$ for $r > h$. These assumptions mean that the equations involving the elements in the $\bar{h}$th column take on one of two forms:

$$\begin{aligned} q_{\bar{r}\bar{h}}\, a_{\bar{h}\bar{h}} &= b_{\bar{r}\bar{h}}, && \text{if } r > h, \\ q_{\bar{r}\bar{h}}\, a_{\bar{h}\bar{h}} + a_{\bar{r}\bar{h}} &= b_{\bar{r}\bar{h}}, && \text{if } r < h. \end{aligned}$$

In case $a_{\bar{h}\bar{h}} = 0$, then $a_{\bar{r}\bar{h}} = b_{\bar{r}\bar{h}}$ for all $r < h$. This is also true for $r > h$, since $a_{\bar{r}\bar{h}} = 0 = b_{\bar{r}\bar{h}}$, so that the $\bar{h}$th columns are the same. By Property 1, $a_{\bar{h}\bar{s}} = 0$ for all s so that $q_{\bar{r}\bar{j}}\, a_{\bar{j}\bar{s}} = \delta_{\bar{r}\bar{j}}\, a_{\bar{j}\bar{s}}$ will hold for all $j \leqslant h$. In addition, $a_{\bar{r}\bar{r}} = 0$ for all $r > h$, by Lemma 1.

If $a_{\bar{h}\bar{h}} \neq 0$, then some $q_{\bar{r}\bar{h}}$ in the first equation must be a unit, since $q_{\bar{j}\bar{j}}$ is the identity element for $j < h$. If it is $q_{\bar{h}\bar{h}}$, then, as before, $a_{\bar{h}\bar{h}} = b_{\bar{h}\bar{h}}$ by Property 3 and $q_{\bar{h}\bar{h}} = 1$. In the second equation $a_{\bar{h}\bar{h}}$ can be replaced by $b_{\bar{h}\bar{h}}$ so that, by Property 4, $a_{\bar{r}\bar{h}} = b_{\bar{r}\bar{h}}$ for all r.

If $q_{\bar{h}\bar{h}}$ were not of degree zero, then some other $q_{\bar{r}\bar{h}}$, $r > h$, must be a unit. We again obtain a contradiction to this assumption from the equation involving the $\bar{r}$th diagonal element of B. In this equation, if $i < h$, then

$$q_{\bar{r}\bar{i}}\, a_{\bar{i}\bar{r}} = \delta_{\bar{r}\bar{i}}\, a_{\bar{i}\bar{r}} = 0$$

by the induction hypothesis. This reduces the equation to the form:

$$\sum_{i \geqslant h} q_{\bar{r}\bar{i}} a_{\bar{i}\bar{r}} = b_{\bar{r}\bar{r}}.$$

We know that

$$d(a_{\bar{i}\bar{r}}) \geqslant d(a_{\bar{i}\bar{i}}) \geqslant d(a_{\bar{h}\bar{h}}) = d(b_{\bar{r}\bar{h}}) \geqslant d(b_{\bar{r}\bar{r}}).$$

In exactly the same manner as before, one of the three inequalities is found to be a true inequality. The only difference lies in using h instead of 1. Therefore this is a false equation and the two columns are identical.

4. Extension of the results. We first note that the Chinese Remainder Theorem **(2**, p. 18**)** holds for a p.i.r.

LEMMA 3. *If m_1 and m_2 are relatively prime elements of a p.i.r., and the $\bar{a}_i$ are any given residue classes modulo m_i, then there exists a residue class $\bar{a}$ modulo m_1m_2 such that $a = a_i$ modulo m_i, for $i = 1,2$.*

Since m_1 and m_2 are relatively prime, in the p.i.r. there exists an f and g such that

$$fm_1 + gm_2 = 1.$$

This means that f is the inverse of m_1 modulo m_2, and similarly that g is the inverse of m_2 modulo m_1. We can now define our desired residue class using the following representative:

$$a = a_1\, gm_2 + a_2 fm_1.$$

That the residue class thus determined has the required properties can be readily verified.

With one more lemma we can outline the extension to the case of the modulus $m = p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$, where the p_i are distinct primes. These prime powers $p_i^{k_i}$ will be called *primary factors* of m. The canonical set we choose will not be easy to describe but it will be unique because the residue class determined in Lemma 3 is unique.

LEMMA 4. *If A and B are row equivalent over $P/\{m\}$, they are row equivalent over $P/\{p^k\}$, where p^k divides m.*

If A and B are row equivalent, then there exists a matrix U such that $UA = B$. Since the determinant of U is a unit in $P/\{m\}$, it must be prime to m. If it is prime to m, it is prime to p^k, and hence is a unit in $P/\{p^k\}$.

The converse of this lemma is not necessarily true, since a number can be prime to p^k and not to m. However, any number that is prime to all primary factors of m is prime to m.

The lemma tells us that all row equivalent matrices over $P/\{m\}$ are row equivalent over $P/\{p^k\}$ for each primary factor of m. For a given class over $P/\{m\}$, there will correspond a row equivalence class over $P/\{p^k\}$. For each of the primary factors of m, the corresponding equivalence class has a canonical representative. One can find by Lemma 3 a matrix over $P/\{m\}$ that is congruent to each of these representatives. This matrix will be row equivalent to the given class over $P/\{m\}$, since it is row equivalent for every divisor of m. We call it the canonical matrix of the given equivalence class.

References

1. L. E. Fuller, *The Hermite canonical form for a matrix with elements in the ring of integers modulo m*, Thesis, University of Wisconsin, 1950.
2. C. C. MacDuffee, *Introduction to abstract algebra* (New York, 1940).