TRANSFORMATION OF BASES FOR RELATIVE LINEAR SETS*

MARGARETE C. WOLF†

The definitions of linear independence, dependence, and extension of sets of vectors relative to a matrix which are used in this paper were recently introduced by M. H. Ingraham,‡ and are not repeated here. The purpose of the present paper is to study the structure of basal elements of a linear extension relative to a matrix. There are developed necessary and sufficient conditions which the elements of a matrix of a transformation must satisfy so that one set of basal elements of a vector space can be transformed into another basal set.

It is assumed throughout this paper that the elements of the matrices and the vectors, as well as the coefficients of the polynomials, are in a field $\mathfrak{F}$. The following theorem is used but stated without proof:§

THEOREM 1. *If $\xi_1, \xi_2, \cdots, \xi_k$ and $\eta_1, \eta_2, \cdots, \eta_l$ are two sets of vectors ($n \times 1$ matrices), each of which is linearly independent relative to an $n \times n$ matrix M, such that $L_M(\xi_1, \xi_2, \cdots, \xi_k) = L_M(\eta_1, \eta_2, \cdots, \eta_l)$, if h_{1i} and h_{2i} are, respectively, the minimum polynomials associated with ξ_i and η_i relative to M, and if g is an irreducible polynomial and t any positive integer, then the number of polynomials h_{1i} divisible by g^t is equal to the number of h_{2i} divisible by g^t.*

This is essentially the only restriction on the polynomials h_{1i} and h_{2i}.

THEOREM 2. *If $\xi_1, \xi_2, \cdots, \xi_k$ is a proper base relative to a matrix M for the space $L_M(\xi_1, \xi_2, \cdots, \xi_k)$, if the minimum polynomial associated with ξ_i relative to M is g^{t_i}, a power of an irreducible polynomial g, and if $\eta_i = \sum_{j=1}^{k} f_{ij}(M)\xi_j$, $(i = 1, 2, \cdots, k)$, where the f_{ij} are polynomials with coefficients in the field $\mathfrak{F}$, necessary and sufficient conditions that the η_i form a proper base relative to M are that the set of polynomials minimally associated with the η_i is exactly the set g^{t_i} in some order, and*

* Presented to the Society, December 29, 1937.

† The work of M. C. Wolf was supported by a grant from the Wisconsin Alumni Research Foundation. The topic was suggested by M. H. Ingraham, who also contributed valuable ideas and criticisms when the paper was presented to a seminar.

‡ M. H. Ingraham and M. C. Wolf, *Relative linear sets and similarity of matrices whose elements belong to a division algebra*, Transactions of this Society, vol. 42 (1937), pp. 16–31.

§ M. H. Ingraham and M. C. Wolf, loc. cit.

that the $k\times k$ *matrix* (f_{ij}) *is of rank* k *in the ring of polynomials reduced modulo* g.

The necessity of the conditions will be proved first. Obviously the minimum polynomial associated with η_i is a power of g; call it g^{s_i}. From Theorem 1 it follows that the set of integers t_i is equal to the set s_i. Let η and ξ be vectors of vectors with η_i and ξ_i, respectively, as the ith element. Let $F=(f_{ij})$ be the matrix with the polynomial f_{ij} in the ith row and jth column, and $F(M)$ the matrix of matrices $(f_{ij}(M))$. The relations $\eta_i=\sum_{j=1}^{k} f_{ij}(M)\xi_j$, $(i=1, 2, \cdots, k)$, can be written as $\eta=F(M)\xi$. A necessary condition that $L_M(\xi_1, \xi_2, \cdots, \xi_k)=L_M(\eta_1, \eta_2, \cdots, \eta_k)$ is that a matrix G exist such that $\xi=G(M)\eta$. Hence it is necessary that G exist such that $\xi=G(M)F(M)\xi$. The matrix GF is square with elements w_{ij}, polynomials with coefficients in $\mathfrak{F}$, and $\xi_i=\sum_{j=1}^{k} w_{ij}(M)\xi_j$. The vectors $\xi_1, \xi_2, \cdots, \xi_k$ are by hypothesis linearly independent relative to M; hence $w_{jj}\equiv 1 \pmod{g^{t_j}}$, and $w_{ij}\equiv 0 \pmod{g^{t_j}}$, $(i\neq j)$. Hence it is necessary that $GF\equiv I \pmod{g}$ and that the determinant $|GF|\equiv 1 \pmod{g}$. The matrices F and G are square; hence $|GF|=|G|\,|F|\equiv 1 \pmod{g}$. Consequently $|F|=|(f_{ij})|\not\equiv 0 \pmod{g}$.

The conditions are sufficient, for if $|F|\not\equiv 0 \pmod{g}$, then for any positive integer t, $(|F|, g^t)=1$, and there exists a polynomial denoted by $|F|^{-1}$, such that $|F|\cdot|F|^{-1}\equiv 1 \pmod{g^t}$. Let $G=|F|^{-1}$ adj F, where adj F is the adjoint of the matrix F. Then $GF\equiv I \pmod{g^t}$. Hence $G(M)F(M)\xi=\xi$; that is, $G(M)\eta=\xi$, and consequently $\eta_1, \eta_2, \cdots, \eta_k$ form a base relative to M for $L_M(\xi_1, \xi_2, \cdots, \xi_k)$. Let g^{s_i} be minimally associated relative to M with η_i, where the set of s_i, $(i=1, 2, \cdots, k)$, is equal to the set of t_i, $(i=1, 2, \cdots, k)$, in some order. The proof that these η_i are linearly independent relative to M is based on the theorem that the number of basal elements in a proper base for a space relative to a field $\mathfrak{F}$ is independent of the base.

From Theorem 1 and from the fact that it is necessary that $|(f_{ij})|\not\equiv 0 \pmod{g}$, the η_i may be rearranged so that the minimum polynomial associated with η_i is g^{t_i}, where $t_1\geqq t_2\geqq \cdots \geqq t_k$. Then η_i is of the form

$$
\begin{aligned}
\eta_i = {} & g^{t_1-t_i}(M)h_{i1}(M)\xi_1 + g^{t_2-t_i}(M)h_{i2}(M)\xi_2 + \cdots \\
& + g^{t_{i-1}-t_i}(M)h_{i\,i-1}(M)\xi_{i-1} \\
& + f_{ii}(M)\xi_i + f_{i\,i+1}(M)\xi_{i+1} + \cdots + f_{ik}(M)\xi_k,
\end{aligned} \tag{1}
$$

where $(f_{ii}, g)=1$. If $t_i>t_{i+1}$, the h_{ij} and the f_{ij} are arbitrary polynomials. However if $t_{i-s-1}>t_{i-s}=t_{i-s+1}=\cdots=t_i>t_{i+1}$, then the principal minor determinant with diagonal elements $f_{i-s\,i-s}, \cdots, f_{i-1\,i-1}, f_{ii}$ cannot be congruent to zero modulo g. Obviously, if the vectors η_i are of the form (1), and if the above conditions on the h_{ij} and f_{ij} are satisfied, the sufficient conditions of Theorem 2 are fulfilled.

THEOREM 3. *If the set of vectors $\xi_1, \xi_2, \cdots, \xi_r$ is a proper base relative to a matrix M for $L_M(\xi_1, \xi_2, \cdots, \xi_r)$, if $\eta_k = \sum_{j=1}^{r} f_{kj}(M)\xi_j$, where the f_{kj} are polynomials with coefficients in $\mathfrak{F}$, and if $\prod_{i=1}^{u} g_i^{t_{ji}}$ and $\prod_{i=1}^{v} g_i^{s_{ki}}$ are minimally associated with ξ_j and η_k, respectively, where the g_i are polynomials irreducible in $\mathfrak{F}$, necessary and sufficient conditions that the η_k form a proper base for $L_M(\xi_1, \xi_2, \cdots, \xi_r)$ are*: (i) *for every i the set of non-zero integers s_{ki} is equal to the set of non-zero t_{ji} in some order,* and (ii) *for every i and for those v_i values of j for which g_i is a factor of the minimum polynomial associated with ξ_j, the v_i columns of (f_{kj}) are of rank v_i in the ring of polynomials reduced modulo g_i.*

Let exactly v_i of the polynomials minimally associated with the ξ_j have a factor g_i. Then as a consequence of Theorem 1 exactly v_i of the polynomials minimally associated with the η_k have a factor g_i. Let $p_i = \prod_{k \neq i} g_k^{c_k}$, where for every value of k the c_k is the maximum value of t_{jk}, $(j = 1, 2, \cdots, r)$.

After a rearrangement of the ξ_j and η_k it may be assumed that $p_i(M)\xi_j = p_i(M)\eta_j = 0$, $(j \geqq v_i + 1)$, and that $p_i(M)\xi_j \neq 0$, $p_i(M)\eta_j \neq 0$, $(j < v_i)$. If polynomials exist such that $\xi_j = \sum_k q_{jk}(M)\eta_k$, then

$$p_i(M)\xi_j = \sum_{k=1}^{v_i} q_{jk}(M)p_i(M)\eta_k.$$

The non-zero $p_i(M)\xi_j$ are linearly independent relative to M for every i. Therefore by Theorem 2 for $k, j = 1, 2, \cdots, v_i$, (f_{kj}) is of rank v_i in the ring of polynomials reduced modulo g_i. If $j \geqq v_i + 1$, then $f_{jk} \equiv 0 \pmod{g_i^{t_{ki}}}$ for $k = 1, 2, \cdots, v_i$, since $(p_i, g_i) = 1$ and since $p_i(M)\eta_j = 0$ when $j \geqq v_i + 1$. For different values of i those v_i columns, which are of rank v_i in the ring of polynomials reduced modulo g_i, may overlap.

That the conditions of the theorem are sufficient for a proper base follows in a similar manner, since a greatest common divisor of the p_i is 1.

The problem of the transformation of bases of relative linear sets is being studied also in the case where $\mathfrak{F}$ is a division algebra, not necessarily commutative.

THE UNIVERSITY OF WISCONSIN