A BASIS THEOREM FOR POLYNOMIAL MODULES

By D. REES

Received 16 March 1955

The purpose of the present note is to prove a basis theorem for polynomial modules (Theorem 1 below). As an application, a proof of the Hilbert function theorem for homogeneous modules (Snapper(1)) is obtained. Both these proofs are elementary in the sense that they do not depend on the decomposition theory for modules over a Noether ring.

DEFINITION. *Let P_n denote the ring $k[X_1, \ldots, X_n]$. where k is a field and $X_1, \ldots, X_n$ are indeterminates over k. A polynomial- or P_n-module is a vector space $\mathfrak{M}$ over k such that, if $u \in \mathfrak{M}$ and if $\phi \in P_n$, a product ϕu is defined, which belongs to $\mathfrak{M}$ and which satisfies:*

$$(1) \quad (\phi+\psi)u = \phi u + \psi u \qquad (\phi, \psi \in P_n,\ u \in \mathfrak{M}),$$

$$(2) \quad \phi(u_1+u_2) = \phi u_1 + \phi u_2 \qquad (\phi \in P_n,\ u_1, u_2 \in \mathfrak{M}),$$

$$(3) \quad 1u = u \qquad (1 \text{ the identity element of } k),$$

$$(4) \quad (\phi\psi)u = \phi(\psi u) \qquad (\phi, \psi \in P_n,\ u \in \mathfrak{M}).$$

$\mathfrak{M}$ is a finite P_n-module if there exist elements $u_1, \ldots, u_r$ in $\mathfrak{M}$ such that every element u of $\mathfrak{M}$ can be expressed in the form

$$u = \sum_{i=1}^{r} \phi_i u_i \quad (\phi_i \in P_n).$$

$u_1, \ldots, u_r$ is termed a module-basis of $\mathfrak{M}$.

In what follows, unless explicitly stated to the contrary, the field k will be assumed to be infinite.

DEFINITION. *Let $Y_i = \sum_{j=1}^{n} a_{ij} X_j$ $(i = 1, \ldots, m)$ be linear forms in $X_1, \ldots, X_n$ over k. We shall term $Y_1, \ldots, Y_m$ independent with respect to $\mathfrak{M}$ if there exists u in $\mathfrak{M}$ such that $\phi(Y_1, \ldots, Y_m)u \neq 0$ if ϕ is not identically zero. Note that this implies that $Y_1, \ldots, Y_m$ are linearly independent.*

DEFINITION. *Let $Y_1, \ldots, Y_m$ be as above. A finite set of elements $w_1, \ldots, w_s$ of $\mathfrak{M}$ will be termed independent over $k[Y_1, \ldots, Y_m]$ if*

$$\sum_{i=1}^{s} \phi_i(Y_1, \ldots, Y_m) w_i = 0$$

implies that ϕ_i is identically zero. The empty set will be considered independent over $k[Y_1, \ldots, Y_m]$, whatever the choice of $Y_1, \ldots, Y_m$, and is the only such set if $Y_1, \ldots, Y_m$ are not independent over $\mathfrak{M}$.

https://doi.org/10.1017/S0305004100030917 Published online by Cambridge University Press

THEOREM 1. *Let $\mathfrak{M}$ be a finite P_n-module. Then there exist linearly independent linear forms $Y_i = \sum_{j=1}^{n} a_{ij}X_j$ $(i = 1, \ldots, n)$ and elements v_{ij} $(i = 0, \ldots, n;\ j = 1, \ldots, t_i)$ of $\mathfrak{M}$ such that every element u of $\mathfrak{M}$ can be expressed in one and only one way in the form*

$$u = \sum_{i=0}^{i=n} \sum_{j=1}^{j=t_i} \phi_{ij}(Y_1, \ldots, Y_{n-i})\, v_{ij}.$$

If, further, $u_1, \ldots, u_r$ is a module-basis of $\mathfrak{M}$, we may choose the elements v_{ij} of the form

$$v_{ij} = \psi_{ij}(X_1, \ldots, X_n)\, u_{k(i,j)},$$

where $\psi_{ij}(X_1, \ldots, X_n)$ is a homogeneous polynomial in $X_1, \ldots, X_n$, and $k(i,j)$ depends on i, j.

We shall proceed by induction on n. First suppose that $n = 0$. Then $P_n = k$, and we may choose $v_{01}, \ldots, v_{0t_0}$ from any module-basis of $\mathfrak{M}$ (in this case, a module-basis of $\mathfrak{M}$ is a set of elements spanning the vector space $\mathfrak{M}$ over k).

Now suppose that $\mathfrak{M}$ is a P_n-module and that the theorem is true for any finite P_m-module, with $m < n$. From the basis $u_1, \ldots, u_r$ choose a subset $v_{01}, \ldots, v_{0t_0}$ which is independent over $P_n = k[X_1, \ldots, X_n]$ and which is maximal with respect to this property ($v_{01}, \ldots, v_{0t_0}$ may be the empty set). Then, if $\mathfrak{M}_1$ denotes the sub-module with $v_{01}, \ldots, v_{0t_0}$ as basis, it follows from the maximal property of $v_{01}, \ldots, v_{0t_0}$ that, for $i = 1, \ldots, r$, there exists a non-zero polynomial $\theta_i(X_1, \ldots, X_n)$ such that

$$\theta_i(X_1, \ldots, X_n)\, u_i \in \mathfrak{M}_1.$$

Hence, if $\theta(X_1, \ldots, X_n) = \prod_{i=1}^{r} \theta_i(X_1, \ldots, X_n)$, $\theta u \in \mathfrak{M}_1$ for all u in $\mathfrak{M}$.

Let $\mathfrak{M}$ be the quotient module $\mathfrak{M}/\mathfrak{M}_1$ and denote the image of an element u of $\mathfrak{M}$ in $\overline{\mathfrak{M}}$ by $\overline{u}$. Then

$$\theta\overline{u} = 0.$$

Now since k is an infinite field we can find $c_1, \ldots, c_{n-1}$ in k such that $\theta^*(c_1, \ldots, c_{n-1}, 1) \neq 0$, where $\theta^*(X_1, \ldots, X_n)$ is the leading form of $\theta(X_1, \ldots, X_n)$, that is, the sum of the terms of highest degree. Let $X_i = Z_i + c_i Z_n$ $(i = 1, \ldots, n-1)$, $X_n = Z_n$. Then $Z_1, \ldots, Z_n$ are also indeterminates over k and $P_n = k[Z_1, \ldots, Z_n]$. Further

$$\theta(X_1, \ldots, X_n) = \chi(Z_1, \ldots, Z_n),$$

where $\chi(Z_1, \ldots, Z_n)$ is of degree, say, N and the coefficient of Z^N is $\theta^*(c_1, \ldots, c_{n-1}, 1)$ and so is a non-zero element of k. From this it follows immediately that $\overline{\mathfrak{M}}$ is a finite $k[Z_1, \ldots, Z_{n-1}]$-module, with basis $Z_n^p \overline{u}_q$ $(p = 0, \ldots, N-1;\ q = 1, \ldots, r)$. We shall denote the elements of this basis by $\overline{w}_1, \ldots, \overline{w}_s$.

By our inductive hypothesis we can now find linearly independent linear forms $Y_1, \ldots, Y_{n-1}$ in $Z_1, \ldots, Z_{n-1}$ and elements $\overline{v}_{ij}$ $(i = 1, \ldots, n;\ j = 1, \ldots, t_i)$ of $\overline{\mathfrak{M}}$ such that each element $\overline{u}$ of $\overline{\mathfrak{M}}$ can be expressed in one and only one way in the form

$$\overline{u} = \sum_{i=1}^{n} \sum_{j=1}^{t_i} \phi_{ij}(Y_1, \ldots, Y_{n-i})\, \overline{v}_{ij}.$$

https://doi.org/10.1017/S0305004100030917 Published online by Cambridge University Press

Hence, if v_{ij} denotes an element of $\mathfrak{M}$ whose image in $\overline{\mathfrak{M}}$ is $\bar{v}_{ij}$ and if u is any element of $\mathfrak{M}$, we can find polynomials $\phi_{ij}(Y_1, \ldots, Y_{n-i})$ such that

$$u_1 = u - \sum_{i=1}^{n} \sum_{j=1}^{t_i} \phi_{ij}(Y_1, \ldots, Y_{n-i})\, v_{ij}$$

belongs to $\mathfrak{M}_1$. Further, the polynomials $\phi_{ij}(Y_1, \ldots, Y_{n-i})$ and hence u_1 are uniquely determined by u. Further, if we write $Y_n = X_n$ then $Y_1, \ldots, Y_n$ are linearly independent and hence $P_n = k[Y_1, \ldots, Y_n]$. Hence the elements $v_{01}, \ldots, v_{0t_0}$ which form a basis of $\mathfrak{M}_1$ are independent over $k[Y_1, \ldots, Y_n]$, and hence we can write u_1 in the form

$$u_1 = \sum_{j=1}^{t_0} \phi_{0j}(Y_1, \ldots, Y_n)\, v_{0j}$$

in one and only one way. Hence we can write

$$u = \sum_{i=0}^{i=n} \sum_{j=0}^{t_i} \phi_{ij}(Y_1, \ldots, Y_{n-i})\, v_{ij}$$

in one and only one way.

Further, by our inductive hypothesis, the elements $\bar{v}_{ij}$ may be taken in the form $\psi^*_{ij}(Z_1, \ldots, Z_{n-1})\, \overline{w}_{k(i,j)}$, where $\psi^*_{ij}(Z_1, \ldots, Z_{n-1})$ is a homogeneous polynomial in $Z_1, \ldots, Z_{n-1}$. Since $\overline{w}_k$ is of the form $X_n^p \overline{u}_q$, it follows immediately that the elements v_{ij} may be chosen to be of the form $\psi_{ij}(X_1, \ldots, X_n)\, u_{k(i,j)}$, where $\psi_{ij}(X_1, \ldots, X_n)$ is a homogeneous polynomial in $X_1, \ldots, X_n$.

For our application of the above theorem we require the notion of a homogeneous polynomial module.

DEFINITION. *A P_n-module $\mathfrak{M}$ is said to be homogeneous if $\mathfrak{M}$ is the direct sum of vector spaces $\mathfrak{M}_k$ $(k = 0, 1, \ldots)$ such that, if $u_k \in \mathfrak{M}_k$ and ϕ_l is a homogeneous polynomial in $X_1, \ldots, X_n$ of degree l, then $\phi_l u_k \in \mathfrak{M}_{k+l}$. The elements of $\mathfrak{M}_k$ are termed homogeneous elements of $\mathfrak{M}$ (of degree k).*

Now suppose that $u_1, \ldots, u_r$ is a module-basis of the homogeneous P_n-module $\mathfrak{M}$. We can write $u_i = \sum_{k=0}^{p} u_{ik}$, where u_{ik} is homogeneous of degree k. The elements u_{ik} $(i = 1, \ldots, r;\ k = 0, \ldots, p)$ also form a module-basis of $\mathfrak{M}$. It follows that a homogeneous P_n-module also possesses a basis consisting of homogeneous elements. It follows therefore that the elements v_{ij} of the last theorem can also be chosen to be homogeneous elements if $\mathfrak{M}$ is homogeneous. With this in mind we can now proceed to the application of Theorem 1 to a proof of the Hilbert function theorem.

THEOREM 2. *Let $\mathfrak{M}$ be a finite homogeneous P_n-module. Let the dimension of the vector space $\mathfrak{M}_q$ be denoted by $H(q)$. Then, for sufficiently large q, $H(q) = \chi(q)$, where $\chi(q)$ is a polynomial in q of degree $\leqslant n-1$.*

By Theorem 1 and the remarks preceding this theorem, we may find linear forms $Y_1, \ldots, Y_n$ in $X_1, \ldots, X_n$ and *homogeneous* elements v_{ij} of $\mathfrak{M}$ such that every element u of $\mathfrak{M}$ is expressible uniquely in the form

$$u = \sum_{i=0}^{n} \sum_{j=0}^{t_i} \phi_{ij}(Y_1, \ldots, Y_{n-i})\, v_{ij}.$$

Now suppose that v_{ij} has degree s_{ij}. Then if $u \in \mathfrak{M}_q$, $\phi_{ij}(Y_1, \ldots, Y_{n-i}) = 0$ if $q < s_{ij}$ and is a homogeneous polynomial of degree $q - s_{ij}$ in $Y_1, \ldots, Y_{n-i}$ if $q \geqslant s_{ij}$. It follows that

https://doi.org/10.1017/S0305004100030917 Published online by Cambridge University Press

$\mathfrak{M}_q$ has as a basis over k the elements $\mu_{ijp}v_{ij}$, where μ_{ijp} ranges over the monomials of degree $q-s_{ij}$ in $Y_1, \ldots, Y_{n-i}$ for each i, j. Now for given i, j the number of such monomials is the binomial coefficient $\binom{q-s_{ij}+n-i-1}{n-i-1}$, where we adopt the convention that $\binom{n}{r} = 0$ if $n < r$. Hence

$$H(q) = \sum_{i=0}^{n} \sum_{j=0}^{t_i} \binom{q-s_{ij}+n-i-1}{n-i-1}.$$

For $q \geqslant \max s_{ij}$, each of the terms on the right-hand side is a polynomial in q and hence, for sufficiently large q, $H(q) = \chi(q)$, where $\chi(q)$ is a polynomial in q of degree $\leqslant n-1$.

DEFINITION. *If $\mathfrak{M}$ is a finite homogeneous P_n-module and $d-1$ is the degree of the polynomial $\chi(q)$ defined above, we term d the dimension of $\mathfrak{M}$.*

If d is the dimension of $\mathfrak{M}$ and if the coefficient of q^{d-1} in $\chi(q)$ is $e(\mathfrak{M})/(d-1)!$, we term $e(\mathfrak{M})$ the multiplicity of $\mathfrak{M}$.

THEOREM 3. (1) *If d is the dimension of $\mathfrak{M}$, there exist d linear forms $Y_1, \ldots, Y_d$ independent with respect to $\mathfrak{M}$ such that $\mathfrak{M}$ is a finite $k[Y_1, \ldots, Y_d]$-module. Further, a set of linear forms independent with respect to $\mathfrak{M}$ contains at most d forms, and if $Z_1, \ldots, Z_r$ are linear forms such that $\mathfrak{M}$ is a finite $k[Z_1, \ldots, Z_r]$-module then $r \geqslant d$.*

(2) *If $Y_1, \ldots, Y_d$ are linear forms independent over $\mathfrak{M}$ such that $\mathfrak{M}$ is a finite $k[Y_1, \ldots, Y_d]$-module, then any set of homogeneous elements of $\mathfrak{M}$ independent over $k[Y_1, \ldots, Y_d]$ which is maximal with respect to this property contains exactly $e(\mathfrak{M})$ elements.*

(1) If d is the dimension of $\mathfrak{M}$, $\chi(q)$ has degree $d-1$. From this it follows, from the formula for $H(q)$, that $t_i = 0$ if $i < n-d$ and $t_{n-d} \neq 0$. Hence if $Y_1, \ldots, Y_d$ are as in Theorem 1, there exists a non-empty subset of $\mathfrak{M}$ independent over $k[Y_1, \ldots, Y_d]$, i.e. $Y_1, \ldots, Y_d$ are independent with respect to $\mathfrak{M}$. Further $\mathfrak{M}$ is a finite $k[Y_1, \ldots, Y_d]$-module, since $t_i = 0$ if $i < n-d$.

Suppose now that $Z_1, \ldots, Z_r$ are independent with respect to $\mathfrak{M}$. Then there exists u in $\mathfrak{M}$ such that $\phi(Z_1, \ldots, Z_r)u \neq 0$ if $\phi(Z_1, \ldots, Z_r) \neq 0$. Further, we may assume that u is homogeneous. Suppose u has degree s. Then if $q > s$, $\mathfrak{M}_q$ contains as a subspace the set of all elements of the form $\phi(Z_1, \ldots, Z_r)u$, where $\phi(Z_1, \ldots, Z_r)$ is a homogeneous polynomial in $Z_1, \ldots, Z_r$ of degree $q-s$. This subspace has dimension $\binom{q-s+r-1}{r-1}$. Hence $\binom{q-s+r-1}{r-1} \leqslant \chi(q)$ for q sufficiently large. Since $\chi(q)$ has degree $d-1$, $r \leqslant d$.

Finally, suppose that $\mathfrak{M}$ is finite $k[Z_1, \ldots, Z_r]$-module. It is clearly a homogeneous $k[Z_1, \ldots, Z_r]$-module. We may further suppose without loss of generality that $Z_1, \ldots, Z_r$ are linearly independent and hence indeterminates over k. Hence it follows from Theorem 2 that $\chi(q)$ has degree at most $r-1$. Hence $r \geqslant d$.

(2) Consider $\mathfrak{M}$ as a $k[Y_1, \ldots, Y_d]$-module and suppose that $u_1, \ldots, u_q$ is a maximal set of homogeneous elements independent over $k[Y_1, \ldots, Y_d]$. We can extend $u_1, \ldots, u_q$ to a homogeneous base of $\mathfrak{M}$ and then choose $u_1, \ldots, u_q$ as the elements $v_{01}, \ldots, v_{0t_0}$ of Theorem 1. Hence $q = t_0$. But as $\chi(q)$ has degree $d-1$, $t_0 = e(\mathfrak{M})$.

https://doi.org/10.1017/S0305004100030917 Published online by Cambridge University Press

We shall conclude this note by considering briefly the effect of removing the restriction that k be infinite in Theorems 1 and 2.

Theorem 1 is not, in general, true if k is finite. However, by using a type of argument due to Uzkov (2) we may obtain the following modification of Theorem 1 valid without restriction on k.

THEOREM 4. *Let $\mathfrak{M}$ be a finite P_n-module. Then there exist polynomials $Y_1, \ldots, Y_n$ in $X_1, \ldots, X_n$ over k and elements v_{ij} $(i = 0, \ldots, n; j = 1, \ldots, t_i)$ such that*

(1) $k[Y_1, \ldots, Y_n] = k[X_1, \ldots, X_n]$,

(2) *every element u of $\mathfrak{M}$ is expressible in one and only one way in the form*

$$u = \sum_{i=0}^{n} \sum_{j=0}^{t_i} \phi_{ij}(Y, \ldots, Y_{n-i}) v_{ij}.$$

Since the proof follows closely that of Theorem 1, we shall only sketch it, indicating in detail where it differs from that proof.

As in the case of Theorem 1, the proof is by induction on n. The case $n = 0$ is identical with the proof in Theorem 1. The proof then follows the proof of Theorem 1 (with, naturally, a different inductive hypothesis) up to the introduction of the subsidiary variables $Z_1, \ldots, Z_n$. In the present theorem we define $Z_1, \ldots, Z_n$ by the equations

$$X_i = Z_i + Z_n^q \quad (i = 1, \ldots, n-1), \quad X_n = Z_n,$$

or

$$Z_i = X_i - X_n^q \quad (i = 1, \ldots, n-1), \quad Z_n = X_n,$$

where q is an integer greater than the maximum exponent of any of the variables $X_1, \ldots, X_n$ in $\theta(X_1, \ldots, X_n)$.

It is clear that $k[Z_1, \ldots, Z_n] = k[X_1, \ldots, X_n]$. Further,

$$\theta(X_1, \ldots, X_n) = \chi(Z_1, \ldots, Z_n),$$

where $\chi(Z_1, \ldots, Z_n)$ has degree N, and the coefficient of Z^N is a non-zero element of k.

The remainder of the proof follows that of Theorem 1, except that $Y_1, \ldots, Y_{n-1}$ are now polynomials in $Z_1, \ldots, Z_{n-1}$ and satisfy $k[Y_1, \ldots, Y_{n-1}] = k[X_1, \ldots, X_{n-1}]$. Y_n is defined by $Y_n = Z_n$ $(= X_n)$, whence $k[Y_1, \ldots, Y_n] = k[X_1, \ldots, X_n]$.

It is clear that Theorem 2 cannot be deduced, in the general case, from Theorem 4 in the same way that Theorem 2 was deduced from Theorem 1 in the case where k is infinite. However, we may deduce Theorem 2 in the case k finite from the case k infinite by the familiar device of adjoining an indeterminate t to k. In this way we obtain a homogeneous module $\mathfrak{M}^*$ over $k(t)[X_1, \ldots, X_n]$ such that the dimension of $\mathfrak{M}_m^*$ over $k(t)$ is equal to that of $\mathfrak{M}_m$ over k. Since $k(t)$ is infinite, Theorem 2 follows for $\mathfrak{M}$ from the corresponding theorem for $\mathfrak{M}^*$.

REFERENCES

(1) SNAPPER, E. Polynomial matrices .... *Amer. J. Math.* 69 (1947), 299–326 and 622–52.

(2) UZKOV, A. I. An algebraic lemma and the normalization theorem of E. Noether. *Mat. Sborn.* (N.S.), 22 (64) (1948), 349–50 (in Russian) and *Math. Rev.* 10 (1949), 97.

DOWNING COLLEGE
CAMBRIDGE

https://doi.org/10.1017/S0305004100030917 Published online by Cambridge University Press