Pacific Journal of Mathematics

# ON THE CONSTRUCTION OF *R*-MODULES AND RINGS WITH POLYNOMIAL MULTIPLICATION

ROSS A. BEAUMONT AND JOHN RICHARD BYRNE

Vol. 7, No. 3 March 1957

# ON THE CONSTRUCTION OF $R$-MODULES AND RINGS WITH POLYNOMIAL MULTIPLICATION

ROSS A. BEAUMONT AND J. RICHARD BYRNE

**1. Introduction.** Let $R$ be a ring and let $R^+$ be the additive group of $R$. If $R^+=S_1\oplus S_2\oplus\cdots\oplus S_n$ is a direct sum of subgroups $S_i$, then each element of $R$ can be written as an $n$-tuple $(s_1, s_2, \cdots, s_n)$, $s_i\in S_i$, $i=1, 2, \cdots, n$, and multiplication in $R$ is given by $n$ mappings

$$f_k: S_1\times S_2\times\cdots\times S_n\times S_1\times S_2\times\cdots\times S_n\to R^+ , \qquad k=1, 2, \cdots, n ,$$

where $f_k(s_1, s_2, \cdots, s_n; t_1, t_2, \cdots, t_n)$ is the $k$-th component of the product $(s_1, s_2, \cdots, s_n)\cdot(t_1, t_2, \cdots, t_n)$. The distributive laws in $R$ imply that the mappings $f_k$ are additive in the first $n$ and in the last $n$ arguments. If $S_1, S_2, \cdots, S_n$ are ideals in $R$, then

$$f_k(s_1, s_2, \cdots, s_n; t_1, t_2, \cdots, t_n)=s_kt_k , \qquad k=1, 2, \cdots, n ,$$

which is a homogeneous quadratic polynomial with integral coefficients in the arguments.

If $R$ is a commutative ring with identity, and if $M$ is a free (left) $R$-module with basis $e_1, e_2, \cdots, e_n$, then $M$ is an algebra over $R$ if and only if there exist elements $\gamma_{ijk}\in R$ such that multiplication in $M$ is defined by

$$\left(\sum_{i=1}^{n} s_ie_i\right)\cdot\left(\sum_{j=1}^{n} t_je_j\right)=\sum_{i,j,k=1}^{n}\gamma_{ijk}s_it_je_k .$$

The $k$-th coordinate of the product,

$$f_k(s_1, s_2, \cdots, s_n; t_1, t_2, \cdots, t_n)=\sum_{i,j=1}^{n}\gamma_{ijk}s_it_j ,$$

is a mapping

$$f_k: \overbrace{R^+\times R^+\times\cdots\times R^+}^{2n}\to R^+$$

which is additive in the first $n$ and last $n$ arguments, and which is a homogeneous quadratic polynomial with coefficients in $R$ in the arguments.

These examples suggest the investigation of polynomial mappings with the indicated additive properties, and a discussion of the problem of constructing $R$-modules and rings which have an additive group which is the direct sum of ideals of a ring $R$, and for which the multiplication

Received October 12, 1956. Presented to the Amer. Math. Soc. October 30, 1954.

is defined by a polynomial mapping.

In § 2 the basic properties of distributive mappings are given. The form of a distributive polynomial mapping is investigated in § 3, and such mappings are characterized in Theorem 2, under the assumption that $R$ is a commutative integral domain. In § 4 and 5 the results of the previous sections are applied to the construction problems mentioned above.

**2. Distributive mappings.** Let $S_1, S_2, \cdots, S_k$ be additive semi-groups with identity 0, and let $M$ be an additive abelian group. Let $f$ be a mapping of $S_1 \times S_2 \times \cdots \times S_k$ into $M$.

DEFINITION. If there exists an integer $m$, where $1 \leq m \leq k$, such that

(i) $$f(s_1+s_1', \cdots, s_m+s_m'; s_{m+1}, \cdots, s_k) = f(s_1, \cdots, s_m; s_{m+1}, \cdots, s_k) + f(s_1', \cdots, s_m'; s_{m+1}, \cdots, s_k),$$

(ii) $$f(s_1, \cdots, s_m; s_{m+1}+s_{m+1}', \cdots, s_k+s_k') = f(s_1, \cdots, s_m; s_{m+1}, \cdots, s_k) + f(s_1, \cdots, s_m; s_{m+1}', \cdots, s_k'),$$

for all $s_i, s_i' \in S_i$, $i=1, 2, \cdots, k$, the mapping $f$ of $S_1 \times S_2 \times \cdots S_k$ into $M$ is called *m-distributive*.

If $k=m$, only (i) of the definition applies, and the mapping $f$ is a homomorphism of $S_1 \oplus S_2 \oplus \cdots \oplus S_k$ into $M$. In the examples given in the introduction, $k=2n$, and the mappings are $n$-distributive.

The following are rather obvious consequences of the definition.

(1) The $m$-distributive mappings of $S_1 \times S_2 \times \cdots \times S_k$ into $M$ form a subgroup $H$ of the additive abelian group $G$ of all mappings of $S_1 \times S_2 \times \cdots \times S_k$ into $M$.

If $M$ is a ring, then the set of mappings $G$ is an $M$-module in the usual way, and the set of $m$-distributive mappings $H$ is a submodule of $G$.

(2) The mappings in $H$ satisfy the relation

$$f(s_1, \cdots, s_m; s_{m+1}, \cdots, s_k) = \sum_{j=m+1}^{k} \sum_{i=1}^{m} f(0, \cdots, 0, s_i, 0, \cdots, 0; 0, \cdots, 0, s_j, 0, \cdots, 0)$$

for all $s_i \in S_i$, $i=1, 2, \cdots, k$.

Statement (2) is proved by induction from (i) and (ii) of the definition.

(3) The mappings in $H$ satisfy

$$f(s_1, \cdots, s_m; 0, \cdots, 0)=f(0, \cdots, 0; s_{m+1}, \cdots, s_k)=0$$

for all $s_i \in S_i$, $i=1, 2, \cdots, k$.

Statement (3) is a generalization of the fact that the distributive laws in a ring imply $a\cdot 0=0\cdot a=0$.

**3. Polynomial functions.** Let $S_1, S_2, \cdots, S_k$ be subsemigroups (not necessarily distinct) of the additive group $R^+$ of a ring $R$, all of which contain the element 0 of $R$. Let $R^*$ be any ring containing $R$, and let

$$f(x_1, x_2, \cdots, x_n)=\sum a_{j_1 j_2 \cdots j_k} x_1^{j_1} x_2^{j_2} \cdots x_k^{j_k}$$

be a polynomial in $R^*[x_1, x_2, \cdots, x_n]$. Then $f$ defines a mapping of $S_1\times S_2\times \cdots \times S_k$ into $R^*$ where

$$f(s_1, s_2, \cdots, s_n)=\sum a_{j_1 j_2 \cdots j_k} s_1^{j_1} s_2^{j_2} \cdots s_k^{j_k}, \qquad s_i \in S_i,\ i=1, 2, \cdots, k .$$

The set $S$ of all such mappings (polynomial functions) is a submodule of the left $R^*$-module $G$ of all mappings of $S_1\times S_2\times \cdots \times S_k$ into $R^*$. As above, we let $H$ be the set of $m$-distributive mappings of $S_1\times S_2\times \cdots \times S_k$ into $R^*$, so that $H$ is a submodule of $G$. Consequently the set of mappings $H \cap S$ is a submodule of $G$.

THEOREM 1. *Each mapping $f \in H \cap S$ is defined by a polynomial of the form*

$$\text{(A)} \qquad f(x_1, x_2, \cdots, x_k)=\sum_{l=m+1}^{k} \sum_{i=1}^{m} \sum_{\substack{j_i, j_l=1 \\ j_i+j_l \leqq t}}^{t-1} a_{j_i j_l}^{(i,l)} x_i^{j_i} x_l^{j_l} .$$

*Proof.* Let $f$ be defined by a polynomial in $R^*[x_1, x_2, \cdots, x_k]$ of degree $t$. Since $f \in H$, we have by (2), Section 2

$$\begin{aligned} f(s_1, s_2, \cdots, s_k) &= \sum_{l=m+1}^{k} \sum_{i=1}^{m} f(0, \cdots, 0, s_i, 0, \cdots, 0; 0, \cdots, 0, s_l, 0, \cdots, 0) \\ &= \sum_{l=m+1}^{k} \sum_{i=1}^{m} \sum_{\substack{j_i, j_l=0 \\ j_i+j_l \leqq t}}^{t} a_{0, \cdots, 0, j_i, 0, \cdots, 0, j_l, 0, \cdots, 0} s_i^{j_i} s_l^{j_l} , \end{aligned}$$

for all $s_i \in S_i$, $i=1, 2, \cdots, k$. The latter expression can be written

$$\sum_{l=m+1}^{k} \sum_{i=1}^{m} \sum_{\substack{j_i, j_l=1 \\ j_i+j_l \leqq t}}^{t-1} a_{0, \cdots, 0, j_i, 0, \cdots, 0, j_l, 0, \cdots, 0} s_i^{j_i} s_l^{j_l}$$

$$+ \sum_{i=1}^{m} \sum_{j_i=1}^{t} a_{0, \cdots, 0, j_i, 0, \cdots, 0} s_i^{j_i}$$

$$+\sum_{l=m+1}^{k}\sum_{j_l=1}^{t} a_{0,\cdots,0,j_l,0,\cdots,0}s_l^{j_l}+a_{0,0,\cdots,0}.$$

By (3), Section 2,

$$0=f(0,\ 0,\ \cdots,\ 0)=a_{0,0,\cdots,0};$$

$$0=f(0,\ \cdots,\ 0,\ s_i,\ 0,\ \cdots,\ 0;\ 0,\ \cdots,\ 0)=a_{0,0,\cdots,0}+\sum_{j_i=1}^{t} a_{0,\cdots,0,j_i,0,\cdots,0}s_i^{j_i}$$

$$=\sum_{j_i=1}^{t} a_{0,\cdots,0,j_i,0,\cdots,0}s_i^{j_i}$$

for all $s_i \in S_i$, $i=1, 2, \cdots, m$;

$$0=f(0,\ \cdots,\ 0;\ 0,\ \cdots,\ 0,\ s_l,\ 0,\ \cdots,\ 0)$$

$$=a_{0,0,\cdots,0}+\sum_{j_l=1}^{t} a_{0,\cdots,0,j_l,0,\cdots,0}s_l^{j_l}$$

$$=\sum_{j_l=1}^{t} a_{0,\cdots,0,j_l,0,\cdots,0}s_l^{j_l}$$

for all $s_l \in S_l$; $l=m+1, \cdots, k$. Denoting $a_{0,\cdots,0,j_i,0,\cdots,0,j_l,0,\cdots,0}$ by $a_{j_i,j_l}^{(i,l)}$, we have

$$f(s_1,\ s_2,\ \cdots,\ s_k)=\sum_{l=m+1}^{k}\sum_{i=1}^{m}\sum_{\substack{j_i,j_l=1\\ j_i+j_l\leqq t}}^{t-1} a_{j_i,j_l}^{(i,l)}s_i^{j_i}s_l^{j_l}$$

for all $s_i \in S_i$, $i=1, 2, \cdots, k$, which completes the proof.

The following examples show that for an arbitrary ring $R$, the converse of Theorem 1 does not hold, and that Theorem 1 is the best possible theorem in the sense that there exist rings for which every polynomial function defined by a polynomial of form (A) is $m$-distributive.

EXAMPLE 1. Let $R=I$, the ring of ordinary integers, let $R^*=R$, and let $S_1=S_2=R^+$. Let $f$: $S_1\times S_2\to R$ be defined by $f(x_1, x_2)=x_1^2x_2$. Then $f$ is defined by a polynomial of form (A) with $m=1$. However $f\notin H$ for $f(1+1;\ 1)=f(2,\ 1)=4$, and $f(1;\ 1)+f(1;\ 1)=1+1=2$.

EXAMPLE 2. Let $R$ be the ring with additive group $R^+=\{u\}$, the cyclic group of order 9, and with multiplication defined by $(iu)\cdot(ju)=3iju$. Then $R$ is a commutative ring [2] such that $R^3=0$, $R^2\neq 0$.

Let $f$ be any mapping of $S_1\times S_2\times\cdots\times S_k$ into an extension $R^*$ of $R$, where $S_1, S_2, \cdots, S_k$ are any subsemigroups of $R^+$ containing 0, such that $f$ is defined by a polynomial of form (A). Then

$$f(s_1, s_2, \cdots, s_k) = \sum_{l=m+1}^{k} \sum_{i=1}^{m} \sum_{\substack{j_i, j_l = 1 \\ j_i + j_l \leqq t}}^{t-1} a_{j_i, j_l}^{(i,l)} s_i^{j_i} s_l^{j_l}$$

$$= \sum_{j=m+1}^{k} \sum_{i=1}^{m} a_{1,1}^{(i,l)} s_i s_l ,$$

since $R^3 = 0$. It is evident that $f$ is $m$-distributive, that is, $f \in H \cap S$.

In the sequel we will be concerned with $m$-distributive polynomial mappings of $S_1 \times S_2 \times \cdots \times S_k$ into $R$. Since a polynomial with coefficients in an extension $R^*$ of $R$ may have its values in $R$, we obtain a larger class of mappings by allowing the coefficients of $f(x_1, x_2, \cdots, x_k)$ to be in $R^* \supseteq R$. For example, polynomials with (ordinary) integral coefficients have values in $R$, and if $R$ does not have an identity, we may consider the coefficients to be in an extension $R^*$ of $R$. Moreover it is a consequence of the theorem that if $R$ is an ideal in $R^*$, then $f$ has values in $R$.

The following lemma is well known (see for example [6, pp. 65–66]), but is given here in the form in which it is most useful for our purposes.

LEMMA. *Let*

$$f = \sum a_{j_1, j_2, \ldots, j_k} x_1^{j_1} x_2^{j_2} \cdots x_k^{j_k} \in R^*[x_1, x_2, \cdots, x_k]$$

*where $R^*$ is a commutative integral domain, and let $f$ be of degree $m_i$ in $x_i$, $i = 1, 2, \cdots, k$. Let $(s_i^{(1)}, s_i^{(2)}, \cdots, s_i^{(n_i)})$ be a set of distinct elements of $R^*$ where $n_i > m_i$, $i = 1, 2, \cdots, k$, such that $f(s_1^{(l_1)}, s_2^{(l_2)}, \cdots, s_k^{(l_k)}) = 0$ for $l_i = 1, 2, \cdots, n_i$, $i = 1, 2, \cdots, k$. Then $f = 0 \in R^*[x_1, x_2, \cdots, x_k]$.*

THEOREM 2. *Let $R^*$ be a commutative integral domain, let $R$ be a subring of $R^*$, and let $S_1, S_2, \cdots, S_k$ be non-zero ideals in $R$. A mapping $f$ from $S_1 \times S_2 \times \cdots \times S_k$ into $R^*$ is in $H \cap S$ if and only if $f$ is defined by a polynomial of the form*

$$\text{(B)} \qquad f(x_1, x_2, \cdots, x_k) = \sum_{l=m+1}^{k} \sum_{i=1}^{m} \sum_{s_i, s_l = 0}^{r} a_{p^{s_i}, p^{s_l}}^{(i,l)} x_i^{p^{s_i}} x_l^{p^{s_l}}$$

*when $R$ has characteristic $p > 0$, and by*

$$\text{(C)} \qquad f(x_1, x_2, \cdots, x_k) = \sum_{l=m+1}^{k} \sum_{i=1}^{m} a_{il} x_i x_l$$

*when $R$ has characteristic zero.*

*Proof.* Let $f$ be defined by a polynomial of form (B) when $R$ has characteristic $p > 0$. Then

$$f(s_1+s_1', \cdots, s_m+s_m'; s_{m+1}, \cdots, s_k)$$

$$= \sum_{l=m+1}^{k} \sum_{i=1}^{m} \sum_{s_i, s_l=0}^{r} a^{(i,l)}_{p^{s_i}, p^{s_l}} (s_i+s_i')^{p^{s_i}} s_l^{p^{s_l}}$$

$$= \sum_{l=m+1}^{k} \sum_{i=1}^{m} \sum_{s_i, s_l=0}^{r} a^{(i,l)}_{p^{s_i}, p^{s_l}} (s_i^{p^{s_i}} + s_i'^{p^{s_i}}) s_l^{p^{s_l}}$$

$$= f(s_1, \cdots, s_m; s_{m+1}, \cdots, s_k) + f(s_1', \cdots, s_m'; s_{m+1}, \cdots, s_k) ,$$

so that $f$ satisfies (i) of the definition for $m$-distributiveness. Similarly (ii) is satisfied, so that $f \in H \cap S$.

It is immediate that a mapping $f$ defined by a polynomial of form (C) is $m$-distributive.

Conversely, we divide the proof into three parts.

1. *$R$ is infinite and has characteristic $p > 0$.*

If $f \in H \cap S$, then $f$ is defined by a polynomial of form (A) by Theorem 1. Then we have for each $i$ $(1 \leq i \leq m)$ and for each $l$ $(m < l \leq k)$,

$$f(0+0, \cdots, s_i+s_i', \cdots, 0+0; 0, \cdots, s_l, \cdots, 0)$$

$$= \sum_{\substack{j_i, j_l=1 \\ j_i+j_l \leq t}}^{t-1} a^{(i,l)}_{j_i, j_l} (s_i+s_i')^{j_i} s_l^{j_l}$$

$$= f(0, \cdots, s_i, \cdots, 0; 0, \cdots, s_l, \cdots, 0)$$

$$+ f(0, \cdots, s_i', \cdots, 0; 0, \cdots, s_l, \cdots, 0)$$

$$= \sum a^{(i,l)}_{j_i, j_l} s_i^{j_i} s_l^{j_l} + \sum a^{(i,l)}_{j_i, j_l} s_i'^{j_i} s_l^{j_l} ,$$

for all $s_i, s_i' \in S_i$, $s_l \in S_l$. Therefore we have the identity

$$\sum_{j_i=2, j_l=1}^{t-1} a^{(i,l)}_{j_i, j_l} \left[ j_i s_i^{j_i-1} s_i' + \frac{j_i(j_i-1)}{2!} s_i^{j_i-2} s_i^2 + \cdots + \frac{j_i(j_i-1)}{2!} s_i^2 s_i'^{j_i-2} + j_i s_i s_i'^{j_i-1} \right] s_l^{j_l} = 0 . \tag{3.1}$$

Since $R$ is an infinite integral domain, each ideal $S_i \neq 0$ is infinite. Therefore the polynomial in $R^*[x, y, z]$ which has the same coefficients as the above expression, vanishes for infinitely many values of each argument $x, y, z$ in $R^*$. By the lemma, each coefficient is zero. Now the coefficient of $x^{j_i-r} y^r z^{j_l}$ $(0 < r < j_i;\ 1 < j_i < t;\ 0 < j_l < t)$ is $\binom{j_i}{r} a^{(i,l)}_{j_i, j_l} = 0$. If $j_i$ is not a power of $p$, then at least one of the binomial coefficients $\binom{j_i}{r}$, $r = 1, 2, \cdots, j_i - 1$, is prime to $p$. Since $R$, and consequently $R^*$, has characteristic $p$, this implies that $a^{(i,l)}_{j_i, j_l} = 0$, for $j_i$ and $j_l$ in the stipu-

lated ranges, whenever $j_i$ is not a power of $p$.

Using (ii) of the definition of an $m$-distributive mapping, a similar argument shows that $a^{(i,l)}_{j_i,j_l}=0$ for $j_i=1, 2, \cdots, t-1$; $j_l=2, 3, \cdots, t-1$ whenever $j_l$ is not a power of $p$.

Since the above argument holds for each $i$ and each $l$, the polynomial of form (A) which defines $f$ has all coefficients zero except for coefficients $a^{(i,l)}_{p^{s_i},p^{s_l}}$, $s_i=0, 1, 2, \cdots$, $s_l=0, 1, 2, \cdots$. Thus $f$ is defined by a polynomial of form (B).

2. *$R$ is finite and has characteristic $p>0$.*

Since $R$ is a commutative integral domain, $R$ is a finite field $GF(p^n)$ and each ideal $S_i\neq 0$ in $R$ is $R$ itself. Since $s^{p^n}=s$ for all $s\in R$, each polynomial function of $S_1\times S_2\times\cdots\times S_k$ into $R^*$ is defined by a polynomial of form (A) of degree at most $p^{n-1}$ in each argument. Since the degree in each argument is less than the number of elements in each $S_i=R$, the lemma can be applied to the identity 3.1, and the proof of 1. is valid in this case also.

3. *$R$ has characteristic zero.*

Since $R$ and each ideal $S_i\neq 0$ in $R$ have infinitely many elements, the proof of 1. can be followed to obtain

$$\binom{j_i}{r}a^{(i,l)}_{j_i,j_l}=0 \qquad \text{and} \qquad \binom{j_l}{r}a^{(i,l)}_{j_i,j_l}=0\ ,$$

for $j_i$, $j_l$, and $r$ in the ranges previously stipulated. Since $R$, and consequently $R^*$, has characteristic zero, this implies that $a^{(i,l)}_{j_i,j_l}=0$ except for $j_i=j_l=1$. Consequently $f$ is defined by a polynomial of form (C).

The following result was obtained in the proof of the theorem.

COROLLARY. *Let $R=GF(p^n)$ and $R^*$ be a commutative integral domain containing $R$. A mapping $f$ of*

$$\overbrace{R\times R\times\cdots\times R}^{k \text{ terms}}$$

*into $R^*$ is in $H\bigcap S$ if and only if $f$ is defined by a polynomial of form* (B) *with $r=n-1$.*

**4. Application to the construction of R-modules.** Let $S\neq 0$ be an ideal in a ring $R$. The set of $(k-1)$-tuples $V=\{(s_2, s_3, \cdots, s_k), s_i\in S\}$ with equality, addition and left scalar multiplication defined componentwise is a left $R$-module. The group of the module is the direct sum

$$\overbrace{S^+\oplus S^+\oplus\cdots\oplus S^+}^{k-1 \text{ terms}}\ .$$

For $r \in R$, $s_i \in S$, the $i$-th component $rs_i$ of the scalar product $r(s_2, s_3, \cdots, s_k)$ is a 1-distributive polynomial function $f$ of the arguments $r; s_2 s_3, \cdots, s_k$. In this section we characterize the most general polynomial function $f$ for which $V=S^+ \oplus S^+ \oplus \cdots \oplus S^+$ is an $R$-module, where $R$ is a commutative integral domain with characteristic zero.

Now $V$ is a left $R$-module if and only if there exists a mapping $f$ from $R \times V$ into $V$ which satisfies the module identities

$$(M_1) \qquad f(r_1, v_1+v_2)=f(r_1, v_1)+f(r_1, v_2) ,$$

$$(M_2) \qquad f(r_1+r_2, v_1)=f(r_1, v_1)+f(r_2, v_1) ,$$

$$(M_3) \qquad f(r_1r_2, v_1)=f(r_1, f(r_2, v_1)) ,$$

for every $r_1, r_2 \in R$ and every $v_1, v_2 \in V$. Denoting the components of $f(r, v)=f(r; s_2, \cdots, s_k)$ by $f_i(r; s_2, \cdots, s_k)$, $i=2, 3, \cdots, k$, we observe that $f$ is given by a set of $k-1$ mappings $f_i$ from

$$\overbrace{R \times S \times S \times \cdots \times S}^{k \text{ terms}}$$

into $S \subseteq R$. Setting $R=S_1$, $S=S_2, \cdots, S=S_k$ to agree with the notation of the preceding sections, the identities $(M_1)$ and $(M_2)$ are just the conditions (i) and (ii) that each mapping $f_i$ be 1-distributive. Interpreting $M_3$ for the components $f_i$ we have

$$(4.1) \qquad f_i(r_1r_2; s_2, \cdots, s_k)=f_i(r_1; f_2(r_2; s_2, \cdots, s_k), \cdots, f_k(r_2; s_2, \cdots, s_k))$$

for every $r_1, r_2 \in R$ and every $s_i \in S$; $i=2, 3, \cdots, k$.

We now assume that $R^*$ is an ideal-preserving extension of $R$, that is, $R^*$ is a ring containing $R$ with the property that if $S$ is an ideal in $R$, then $S$ is an ideal in $R^*$. For example, there exists a ring with identity containing $R$ which is an ideal-preserving extension of $R$. Let $f_i$, $i=2, 3, \cdots, k$, be a mapping from $R \times V$ into $R^*$ defined by a polynomial

$$(4.2) \qquad f_i(x_1; x_2, \cdots, x_k)=\sum a_{j_1 j_2 \cdots j_k} x_1^{j_1} x_2^{j_2} \cdots x_k^{j_k}$$

with coefficients in $R^*$. Denote the system consisting of the group $V$ and the mappings $f_i$ defined by (4.2) by $(V, f_i)$. We obtain the following application of Theorem 2.

THEOREM 3. *Let $R^*$ be a commutative integral domain with characteristic zero which is an ideal-preserving extension of $R$. Then $(V, f_i)$ is a left $R$-module with scalar multiplication defined by $r \cdot (s_2, s_3, \cdots, s_k)=(f_2, f_3, \cdots, f_k)$ if and only if each $f_i$ is defined by a polynomial of the form*

(4.3) $$f_i(x_1; x_2, \cdots, x_k) = \sum_{l=2}^{k} a_l^{(i)} x_1 x_l , \qquad a_l^{(i)} \in R^* ,$$

*such that the matrix* $A=(a_l^{(i)})$ *is idempotent; that is* $r\cdot(s_2, s_3, \cdots, s_k) = r(s_2, s_3, \cdots, s_k)A'$, *where the right member is an ordinary matrix product in which* $A'$ *is the transpose of the matrix* $A$.

*Proof.* If $(V, f_i)$ is a left $R$-module, then by the foregoing discussion, the mappings $f_i$ are 1-distributive polynomial mappings with values in $S \subseteq R^*$. By Theorem 2, with $S_1=R$, $S_2=S_3=\cdots=S_k=S$, and $m=1$, each $f_i$ is defined by a polynomial of form (C)

$$f_i(x_1; x_2, \cdots, x_k) = \sum_{l=2}^{k} a_{1l}^{(i)} x_1 x_l = \sum_{l=2}^{k} a_l^{(i)} x_1 x_l .$$

Since each $f_i$ must satisfy the identity (4.1) we have

$$\sum_{l=2}^{k} a_l^{(i)} (r_1 r_2) s_l = \sum_{l=2}^{k} a_l^{(i)} r_1 \left[ \sum_{j=2}^{k} a_j^{(l)} r_2 s_j \right]$$

$$= \sum_{l=2}^{k} \sum_{j=2}^{k} a_j^{(i)} a_l^{(j)} r_1 r_2 s_l ,$$

for every $r_1, r_2 \in R$ and every $s_l \in S$. This implies $a_l^{(i)} = \sum_{j=2}^{k} a_j^{(i)} a_l^{(j)}$ or that the matrix $A=(a_l^{(i)})$ is idempotent. Since

$$f_i(r; s_2, \cdots, s_k) = \sum_{l=2}^{k} a_l^{(i)} rs = r \sum_{l=2}^{k} a_l^{(i)} s_l ,$$

we have $r\cdot(s_2, \cdots, s_k) = r(s_2, \cdots, s_k)A'$ where the right member is an ordinary matrix product.

Conversely, it is readily observed that if $f_i$ is defined by (4.3) with $A=(a_l^{(i)})$ idempotent, then $f_i$ has values in $S$ since $S$ is an ideal in $R^*$, $f_i$ is 1-distributive, and $f_i$ satisfies (4.1). Therefore $(V, f_i)$ is a left $R$-module.

If we specialize to the case where $R=F$ is a field, we have $S_2=S_3=\cdots=S_k=F$ and $R^*=F$, so that $(V, f_i)$ is the group of $(k-1)$-tuples with elements in $F$ for which scalar multiplication is defined by (4.2). Theorem 3 characterizes the $(V, f_i)$ which are $F$-modules, and we let $(V, A)$ denote the $F$-module $(V, f_i)$ with scalar multiplication defined by (4.3) where $A=(a_l^{(i)})$ is idempotent. Let $E_m = \begin{pmatrix} I_m & 0 \\ 0 & 0 \end{pmatrix}$, where $0 \leq m \leq k-1$. The following theorem completely classifies the $F$-modules $(V, f_i)$.

THEOREM 4. *The left* $F$*-module* $(V, A)$ *is* $F$*-isomorphic to the* $F$*-module* $(V, E_m)$ *for some* $m$, $0 \leq m \leq k-1$. *Moreover* $(V, E_m)$ *is not* $F$*-isomorphic to* $(V, E_n)$ *if* $m \neq n$.

*Proof.* If $A$ is similar to $B$, then $(V, A)$ is $F$-isomorphic to $(V, B)$. For in $(V, A)$,

$$r\cdot(s_2, s_3, \cdots, s_k)=r(s_2, s_3, \cdots, s_k)A' ,$$

and in $(V, B)$,

$$r\cdot(s_2, s_3, \cdots, s_k)=r(s_2, s_3, \cdots, s_k)B'=r(s_2, s_3, \cdots, s_k)PA'P^{-1}$$

for some non-singular matrix $P$. The mapping $\varphi$ defined by

$$\varphi[(s_2, s_3, \cdots, s_k)]=(s_2, s_3, \cdots, s_k)P^{-1}$$

is an $F$-isomorphism.

Since $A$ is idempotent, $A$ is similar to $E_m$ for some $m$, $0\leq m\leq k-1$ [1, p. 88], which completes the proof of the first part of the theorem.

In $(V, E_m)$,

$$r\cdot(s_2, s_3, \cdots, s_k)=(rs_2, rs_3, \cdots, rs_{m+1}, 0, \cdots, 0) ,$$

so that the submodule $1\cdot(V, E_m)=(s_2, s_3, \cdots, s_{m+1}, 0, \cdots, 0)$ is the vector space over $F$ of dimension $m$. Any $F$-isomorphism of $(V, E_m)$ onto $(V, E_n)$ induces an $F$-isomorphism of $1\cdot(V, E_m)$ onto $1\cdot(V, E_n)$, but if $m\neq n$ these submodules cannot be $F$-isomorphic since they are vector spaces of different dimensions over $F$.

COROLLARY. *The $F$-modules $(V, A)$ and $(V, B)$ are $F$-isomorphic if and only if $A$ and $B$ have the same rank.*

In the above discussion, the $(V, f_i)$ were all $(k-1)$-tuples for a fixed $k$. We now consider $(V_k, f_i)$ and $(V_l, f_i)$, $k\neq l$. By Theorem 4, it is sufficient to consider $(V_k, E_m)$, $0\leq m\leq k-1$ and $(V_l, E_n)$, $0\leq n\leq l-1$.

THEOREM 5. *The $F$-modules $(V_k, E_m)$ and $(V_l, E_n)$ are $F$-isomorphic if and only if $m=n$ and either $k=l$ or $F^+$ has infinite rank.*[1]

*Proof.* Suppose first that $\varphi$ is an $F$-isomorphism of $(V_k, E_m)$ onto $(V_l, E_n)$. Then as in Theorem 4, $1\cdot(V_k, E_m)$ and $1\cdot(V_l, E_n)$ are $F$-isomorphic vector spaces of dimension $m$ and $n$ respectively over $F$. Hence $m=n$. Assume that $k\neq l$, and let $M$ and $N$ be the submodules of $(V_k, E_m)$ and $(V_l, E_m)$ respectively which are annihilated by $1\in F$. Then $\varphi$ induces an isomorphism of $M$ onto $N$ as additive groups.

$$M=\{(0, \cdots, 0, s_{m+1}, \cdots, s_{k-1}), s_i\in F\}=\overbrace{F^+\oplus\cdots\oplus F^+}^{k-1-m}$$

[1] The additive group $F^+$ of a field $F$ of characteristic 0 is a divisible torsion-free group and therefore is the direct sum of $\alpha$ copies of the additive group of rational numbers. The cardinal number $\alpha$, which is an invariant, is called the rank of $F^+$ [4, pp. 10–11].

and

$$N=\{(0, \cdots, 0, s_{m+1}, \cdots, s_{l-1}), s_i \in F\}=\overbrace{F^+ \oplus \cdots \oplus F^+}^{l-1-m}.$$

If $F^+$ has finite rank, then $M$ and $N$ have different rank, and are not isomorphic. Hence $F^+$ has infinite rank.

Conversely, if $m=n$ and $k=l$, there is nothing to prove. Suppose, then, that $m=n$ and that $F^+$ has infinite rank. Now $(V_k, E_m)=1\cdot(V_k, E_m)\oplus M$ and $(V_l, E_m)=1\cdot(V_l, E_m)\oplus N$, where $M$ and $N$ each have the decomposition into a direct sum of copies of $F^+$ given above. Since $F^+$ has infinite rank, $M$ and $N$ have the same rank and are isomorphic as additive groups. But since $F$ annihilates $M$ and $N$, this isomorphism is an $F$-isomorphism. Finally, $1\cdot(V_k, E_m)$ is $F$-isomorphic to $1\cdot(V_l, E_m)$ since they are vector spaces of the same dimension.

**5. Application to the construction of rings.** As in the previous section, we let $S\neq 0$ be an ideal in a ring $R$ and consider the set of $n$-tuples $V=\{(s_1, s_2, \cdots, s_n), s_i \in S\}$ with equality and addition defined componentwise. Now $V$ is a ring if and only if there exists a mapping $f$ from $V\times V$ into $V$ which satisfies

$(R_1)$ $$f(v_1+v_2, v_3)=f(v_1, v_3)+f(v_2, v_3)$$

$(R_2)$ $$f(v_1, v_2+v_3)=f(v_1, v_2)+f(v_1, v_3)$$

$(R_3)$ $$f(f(v_1, v_2), v_3)=f(v_1, f(v_2, v_3))$$

for every $v_1, v_2, v_3 \in V$.

Denoting the components of $f(v_1, v_2)=f(s_1, \cdots, s_n; t_1, \cdots, t_n)$ by $f_i(s_1, \cdots, s_n; t_1, \cdots, t_n)$, $i=1, 2, \cdots, n$, $f$ is given by a set of $n$ mappings $f_i$ from

$$\overbrace{S\times S\times \cdots \times S}^{2n \text{ terms}}$$

into $S\subseteqq R$. The identities $R_1$ and $R_2$ are just the conditions (i) and (ii) that each mapping $f_i$ be $n$-distributive. In this application, $k=2n$, and $S_i=S$, $i=1, 2, \cdots, k$ in the notation of § 2. Interpreting $R_3$, the associative law, for the components $f_i$, we obtain

$$(5.1)\quad f_i(f_1(s_1, \cdots, s_n; t_1, \cdots, t_n), \cdots, f_n(s_1, \cdots, s_n; t_1, \cdots, t_n); u_1, \cdots, u_n)$$
$$=f_i(s_1, \cdots, s_n; f_1(t_1, \cdots, t_n; u_1, \cdots, u_n), \cdots, f_n(t_1, \cdots, t_n; u_1, \cdots, u_n))$$

for every $s_i, t_j, u_k \in S$.

We assume that $R^*$ is an ideal-preserving extension of $R$ and that each $f_i$, $i=1, 2, \cdots, n$ is defined by a polynomial

$$(5.2) \qquad f_i(x_1, \cdots, x_n; y_1, \cdots, y_n) = \sum a_{j_1 \cdots j_n k_1 \cdots k_n} x_1^{j_1} \cdots x_n^{j_n} y_1^{k_1} \cdots y_n^{k_n}$$

with coefficients in $R^*$. Denote the system consisting of the group $V$ and the mappings $f_i$ defined by (5.2) by $(V, f_i, n)$. We obtain the following application of Theorem 2.

THEOREM 6. *Let $R^*$ be a commutative integral domain which is an ideal preserving extension of $R$. Then $(V, f_i, n)$ is a ring with multiplication defined by $(s_1, \cdots, s_n)\cdot(t_1, \cdots, t_n)=(f_1, \cdots, f_n)$ if and only if each $f_i$, $i=1, 2, \cdots, n$ satisfies* (5.1) *and is defined by a polynomial of the form*

$$(5.3) \qquad f_i(x_1, \cdots, x_n; y_1, \cdots, y_n) = \sum_{l=1}^{n} \sum_{j=1}^{n} \sum_{s_j, s_l=0}^{r} {}^{(i)}a_{s_j s_l}^{(j,l)} x_j^{p^{s_j}} y_l^{p^{s_l}} ,$$

*or*

$$(5.4) \qquad f_i(x_1, \cdots, x_n; y_1, \cdots, y_n) = \sum_{l=1}^{n} \sum_{j=1}^{n} a_{jl}^{(i)} x_j y_l ,$$

*according as $R$ has characteristic $p>0$ or 0.*

*Proof.* If $(V, f_i, n)$ is a ring, then we have observed above that the mappings $f_i$ are $n$-distributive mappings with values in $S \subseteq R^*$. Since the $f_i$ are polynomial mappings into $R^*$, it follows from Theorem 2, that they are defined by polynomials of form (B) or (C) according as the characteristic of $R$ is $p>0$ or 0. We have seen that the associative law implies (5.1).

Conversely, if multiplication in $(V, f_i, n)$ is defined by $(s_1, \cdots, s_n)\cdot(t_1, \cdots, t_n)=(f_1, \cdots, f_n)$, where each $f_i$ is defined by (5.3) or (5.4) according as the characteristic of $R$ is $p>0$ or 0, then by Theorem 2, each $f_i$ is $n$-distributive. Thus, multiplication in $(V, f_i, n)$ is distributive with respect to addition. Since each $f_i$ satisfies (5.1), multiplication is associative, and $(V, f_i, n)$ is a ring.

EXAMPLE 3. Let $R$ be a field $F$ with characteristic zero. Then $R^*=F$, $S=F$, and $(V, f, 1)$ is the group $F^+$ and the mapping $f$ defined by $f(x; y)=\sum a_{jk}x^j y^k$, $a_{jk} \in F$. By Theorem 6, $(V, f, 1)$ is a ring with multiplication defined by $s\cdot t=\sum a_{jk}s^j t^k$ only if $f$ is defined by $f(x; y)=axy$, $a \in F$. If $a \neq 0$, $(V, f, 1)$ is isomorphic to $F$ under the correspondence $sa^{-1} \leftrightarrow s$, so that we can conclude that the only non-trivial rings with additive group $F^+$ and with multiplication defined by a polynomial function of $F \times F$ into $F$ are fields isomorphic to $F$ [3, p. 177].

EXAMPLE 4. Let $R$ be the finite field $GF(3^2)$. Then $R^*=GF(3^2)$,

$S=GF(3^2)$, and $(V, f, 1)$ is a ring only if multiplication is defined by (see the Corollary to Theorem 2).

$$s\cdot t=f(s;\ t)=a_{00}st+a_{01}st^3+a_{10}s^3t+a_{11}s^3t^3\ , \qquad a_{ij}\in GF(3^2)\ .$$

Selecting $a_{00}=a_{10}=1$, $a_{01}=a_{11}=0$, $f(s;\ t)=st+s^3t$, and $f(s;\ t)$ satisfies (5.1). Hence $(V, f, 1)$ is a ring. Let $\xi$ be the primitive eighth root of unity which generates the multiplicative group of $GF(3^2)$. Then $\xi^2\cdot 1=f(\xi^2;\ 1)$ $=\xi^2+\xi^6=\xi^2(1+\xi^4)=0$. Hence $(V, f, 1)$ has zero divisors, and in this case we have an example of a non-trivial ring with additive group $GF(3^2)^+$ and with polynomial multiplication which is not isomorphic to $GF(3^2)$.

It should be remarked in conclusion, that when $R$ has characteristic zero and $(V, f_i, n)$ is a ring, the multiplication rule (5.4) is the same as that for an algebra over $R^*$ (see Introduction); and if $R^*$ has an identity, $(V, f_i, n)$ can be regarded as a subalgebra of an ordinary algebra of dimension $n$ over $R^*$. Hence the coefficients $a_{jl}^{(i)}$ of the polynomials $f_i$ play the same role as the multiplication constants of an algebra, and the associative law (5.1) can be interpreted as a matrix identity [5, p. 294].

## REFERENCES

1. A. A. Albert, *Modern Higher Algebra*, Chicago, 1937.
2. Ross A. Beaumont, *Rings with additive group which is the direct sum of cyclic groups*, Duke Math. J., **15** (1948), 367-369.
3. ——— and H. S. Zuckerman, *A characterization of the subgroups of the additive rationals*, Pacific J. Math. **1** (1951), 169-177.
4. Irving Kaplansky, *Infinite Abelian Groups*, University of Michigan Press, 1954.
5. C. C. MacDuffee, *Modules and ideals in a Frobenius algebra*, Monatsh. Math. Phys., **48** (1939), 293-313.
6. B. L. van der Waerden, *Modern Algebra*, New York, 1949.

UNIVERSITY OF WASHINGTON AND PORTLAND STATE COLLEGE

# PACIFIC JOURNAL OF MATHEMATICS

## EDITORS

H. L. ROYDEN
Stanford University
Stanford, California

A. L. WHITEMAN
University of Southern California
Los Angeles 7, California

R. A. BEAUMONT
University of Washington
Seattle 5, Washington

E. G. STRAUS
University of California
Los Angeles 24, California

## ASSOCIATE EDITORS

E. F. BECKENBACH
C. E. BURGESS
M. HALL
E. HEWITT
A. HORN
V. GANAPATHY IYER
R. D. JAMES
M. S. KNEBELMAN
L. NACHBIN
I. NIVEN
T. G. OSTROM
M. M. SCHIFFER
G. SZEKERES
F. WOLF
K. YOSIDA

## SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
OREGON STATE COLLEGE
UNIVERSITY OF OREGON
UNIVERSITY OF SOUTHERN CALIFORNIA
STANFORD UNIVERSITY
UNIVERSITY OF UTAH
WASHINGTON STATE COLLEGE
UNIVERSITY OF WASHINGTON
* * *
AMERICAN MATHEMATICAL SOCIETY
CALIFORNIA RESEARCH CORPORATION
HUGHES AIRCRAFT COMPANY
THE RAMO-WOOLDRIDGE CORPORATION


---

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any of the editors. All other communications to the editors should be addressed to the managing editor, E. G. Straus at the University of California, Los Angeles 24, California.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

---


The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. The price per volume (4 numbers) is $12.00; single issues, $3.50. Back numbers are available. Special price to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues, $1.25.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 2120 Oxford Street, Berkeley 4, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 10, 1-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

**Pacific Journal of Mathematics**
Vol. 7, No. 3 March, 1957

Silvio Aurora, *Multiplicative norms for metric rings* . . . . . 1279
Ross A. Beaumont and John Richard Byrne, *On the construction of R-modules and rings with polynomial multiplication* . . . . . 1305
Fred Brafman, *An ultraspherical generating function* . . . . . 1319
Howard Ernest Campbell, *On the Casimir operator* . . . . . 1325
Robert E. Edwards, *Representation theorems for certain functional operators* . . . . . 1333
Tomlinson Fort, *The five-point difference equation with periodic coefficients* . . . . . 1341
Isidore Heller, *On linear systems with integral valued solutions* . . . . . 1351
Harry Hochstadt, *Addition theorems for solutions of the wave equation in parabolic coordinates* . . . . . 1365
James A. Hummel, *The coefficient regions of starlike functions* . . . . . 1381
Fulton Koehler, *Estimates for the eigenvalues of infinite matrices* . . . . . 1391
Henry Paul Kramer, *Perturbation of differential operators* . . . . . 1405
R. Sherman Lehman, *Development of the mapping function at an analytic corner* . . . . . 1437
Harold Willis Milnes, *Convexity of Orlicz spaces* . . . . . 1451
Vikramaditya Singh, *Interior variations and some extremal problems for certain classes of univalent functions* . . . . . 1485
William Lee Stamey, *On generalized euclidean and non-euclidean spaces* . . . . . 1505
Alexander Doniphan Wallace, *Retractions in semigroups* . . . . . 1513
R. L. Wilder, *Monotone mappings of manifolds* . . . . . 1519