ANNALI DELLA
SCUOLA NORMALE SUPERIORE DI PISA
Classe di Scienze

H. G. MOORE
ADIL YAQUB

An existence theorem for semi-primal algebras

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 3^e série, tome 22, n^o 4 (1968), p. 559-570

<http://www.numdam.org/item?id=ASNSP_1968_3_22_4_559_0>

AN EXISTENCE THEOREM FOR SEMI-PRIMAL ALGEBRAS

by H. G. MOORE and ADIL YAQUB(*)

The theory of a primal algebra subsumes and substantially generlizes the classical Boolean theory as well as that of p-rings and Post algebras. Here a primal algebra is essentially a finite algebra in which each map is expressible in terms of the primitive operations of the algebra. Recently, Foster and Pixley showed that the primal algebras themselves, in turn, are subsumed by the class of semi-primal algebras, and a general structure theory for these semi-primal algebras was then established.

The horizon of new applications of this general structure theory greatly depends, of course, on the discovery of classes of semi-primal algebras (other than the primal ones). In this paper, we show that a large class of binary algebras, called z-algebras, endowed with a suitably chosen (but nevertheles quite general) permutation, yields semi-primal algebras (of species (2,1)). (See Theorem 2.2). We then lean heavily on this result to prove that *any* finite ring R with identity, and of characteristic different from two, can always be endowed with a permutation $\frown$ such that $(R, \times, \frown)$ is semi-primal. (See Theorem 3.2). We also show (by means of counter-examples) that this result need not be true for rings of characteristic two.

1. Fundamental concepts and lemmas.

We recall the basic concepts of [1] and [2]. Let $\mathfrak{A} = (A, \Omega)$ be a universal algebra of species S, $S = (n_1, n_2, \ldots)$ where the n_i are non-negative

---

(*) The work of this author was supported, in part, by National Science Foundation Grants GP 4163 and GP 5929.

Pervenuto alla Redazione il 9 Gennaio 1968.

integers and let $\mathfrak{o}_1, \mathfrak{o}_2, \ldots$ denote the primitive operations in Ω where $\mathfrak{o}_i$ is an n_i-ary operation on A. By an *S-exepression* $\Phi(\xi_1, \ldots)$ we mean a primitive composition of free symbols $-\xi_1 \ldots -$ via the primitive operations $\mathfrak{o}_i$. When two algebras $\mathfrak{A}$ and $\mathfrak{A}'$ are of the same species, we identify the two sets of operations Ω and Ω', and use the same operation symbols. A (set-theoretic) function $f(\xi_1, \ldots \xi_k)$ from $A \times \ldots \times A$ into A is said to be *expressible* if there exists an S-expression Φ such that $f = \Phi$ on A; i.e., Φ yelds f when members of A are substituted for the free symbols in Φ. An A-function $f(\xi_1, \xi_2, \ldots)$ is called *conservative* if for every subalgebra $\mathfrak{A}_i = (A_i, \Omega)$ of $\mathfrak{A}$, $f(\alpha, \beta, \ldots) \in A_i$ whenever $\alpha, \beta, \ldots \in A_i$. A *finite* algebra $\mathfrak{A}$ different from the one-element algebra $\mid$ is called *primal* if every A-function is expressible, while $\mathfrak{A}$ is called *semi-primal* if every conservative A-function is expressible. If $\mathfrak{A}$ is semi-primal and possesses exactly one subalgebra $\mathfrak{C}(\neq \mathfrak{A})$, then $\mathfrak{A}$ is called a *subprimal* algebra, and $\mathfrak{C}$ is called the *core* of $\mathfrak{A}$. If $\mathfrak{C}$ has more than one element, $\mathfrak{A}$ is a *regular subprimal*; otherwise, it is a *singular subprimal.*

The principal results of the theory of semi-primals are sumarized for convenience in the following theorem (see [2]).

LEMMA 1.1. *Let $\mathfrak{B}$ be a semi-primal algebra. Then*

(i) *Each minimal subalgebra is either primal or the one element subalgebra* $\mid$.

(ii) *$\mathfrak{B}$ is simple. Also, any subalgebra of $\mathfrak{B}(\neq \mid)$ is again semiprimal and therefore simple.*

(iii) *$\mathfrak{B}$ possesses no non-identical automorphism.*

In a universal algebra $\mathfrak{A} = (A, \Omega)$ of species S, an element α is said to be *expressible* if there exists an S-expression $\varrho_\alpha(\xi)$ such that $\varrho_\alpha(\xi) = \alpha$ for all $\xi \in \mathfrak{A}$. For a subprimal algebra, the set of all expressible elements coincides with its core [2; Theorem 8.4]. We say that $\mathfrak{A}$ possesses a *frame*

$$[0, 1, \times, \frown, \smile]$$

if there exist two distinguished elements 0, $1 \in A$ $(0 \neq 1)$ and operations $\times$ (binary), $\frown$ (unary), and $\smile$ (unary) such that

(1) 0 and 1 are expressible;

(2) $\xi \times \eta$, $\xi\frown$, and $\xi\smile$ are all expressible;

(3) $\xi\frown$ and $\xi\smile$ are permutations of A with $\xi\smile$ the inverse of $\xi\frown$; and

(4) $0 \times \eta = \eta \times 0 = 0$, $1 \times \eta = \eta \times 1 = \eta$ for all $\eta \in A$; and $0\frown = 1$.

We shall also make use of the characterization of regular subprimal algebras given by the following theorem of Foster and Pixley [2; Theorem

9.1]. Note that $\mathfrak{A} \setminus \mathfrak{C}$ denotes the set of all elements of $\mathfrak{A}$ which are not in $\mathfrak{C}$.

LEMMA 1.2. *For an algebra $\mathfrak{A} = (A, \Omega)$ of species S to be a regular subprimal, it is necessary and sufficient that*

(i) $\mathfrak{A}$ *be a finite algebra of at least three elements.*

(ii) $\mathfrak{A}$ *possess precisely one subalgebra $\mathfrak{C} (\neq \mathfrak{A})$ — the core of $\mathfrak{A}$.*

(iii) $\mathfrak{A}$ *possess a frame.*

(iv) *For each $\alpha \in \mathfrak{A}$ the characteristic function $\delta_\alpha(\xi)$ (defined below) is expressible.*

(v) *There exists a non-core element $\lambda \in \mathfrak{A} \setminus \mathfrak{C}$ which is « ex-expressible »,* i. e., *for a suitable S expression $\varrho_\lambda(\xi)$ we have $\varrho_\lambda(\xi) = \lambda$ for all $\xi \in \mathfrak{A} \setminus \mathfrak{C}$.*

The characteristic function $\delta_\alpha(\xi)$, where $\alpha \in \mathfrak{A}$, is defined by

$$\delta_\alpha(\xi) = \begin{cases} 1 \text{ if } \xi = \alpha \\ 0 \text{ if } \xi \neq \alpha \end{cases}, \qquad \text{(for all } \xi \in \mathfrak{A}\text{)}.$$

It now seems convenient to introduce the following

NOTATION 1.1. For any positive integer q, we define

$$\xi^{\frown q} = \text{ def } = (\ldots((\xi^{\frown})\ldots)^{\frown},$$

q interations; $\xi^{\smile q}$ is defined similarly. Moreover, we define

$$a \prec_{\frown} b = (a^{\frown} \times b^{\frown})^{\smile}, \quad (\xi^{\smile} \text{ is the inverse of } \xi^{\frown}).$$

Observe that

$$a \prec_{\frown} 0 = 0 \prec_{\frown} a = a.$$

2. Main Theorems.

In preparation for the proofs of our main theorems, we first recall the following

DEFINITION 2.1 A *binary algebra* is an algebra $(B, \times)$ of species (2) possessing elements 0, 1 $(0 \neq 1)$ such that

$$a \prec 0 = 0 \cdot a = 0, \; a \cdot 1 = 1 \cdot a = a, \quad \text{for all } a \text{ in } B.$$

We now have the following

THEOREM 2.1 *Suppose* $(B, \times)$ *is a finite binary algebra which has exactly* n *elements,* $n \geq 3$, *and suppose* $(B^*, \times)$ *is a subalgebra of* $(B, \times)$, *where* $B^* = \{0, 1\}$. *Suppose* $\widehat{\ }$ *is a permutation of* B *such that* $0\widehat{\ } = 1$ *and* $1\widehat{\ } = 0$. *If for some* $b \in B \setminus B^*$ *the characteristic function* $\delta_b(\xi)$ *is* $(\times, \widehat{\ }, \breve{\ })$*-expressible, then (see Notation* 1.1)

(i) b *is ex-expressible,* i. e., *for each* $\xi \in B \setminus B^*$,

$$(2.1)\quad b = \varrho_b(\xi) = [\xi\widehat{\ }\,\delta_b(\xi\widehat{\ })] \times_{\frown} [\xi\widehat{\ }^2\,\delta_b(\xi\widehat{\ }^2)] \times_{\frown} \dots \times_{\frown} [\xi\widehat{\ }^{n-2}\,\delta_b(\xi\widehat{\ }^{n-2})],$$

with any association of the $\widehat{\ }$*-factors.*

(ii) *For every* $\xi \in B$ *and any association of the* $\widehat{\ }$*-factors,*

$$(2.2)\qquad \delta_1(\xi) = \xi^2[\delta_b(\xi\widehat{\ }) \times_{\frown} \delta_b(\xi\widehat{\ }^2) \times_{\frown} \dots \times_{\frown} \delta_b(\xi\widehat{\ }^{n-2})]\widehat{\ },$$

and hence $\delta_1(\xi)$ *is* $(\times, \widehat{\ }, \breve{\ })$*-expressible.*

$$(iii)\qquad \delta_0(\xi)\,\delta_1(\xi) = 0,\ (\delta_0(\xi)\,\delta_1(\xi))\widehat{\ } = 1,$$

and hence both 0 *and* 1 *are* $(\times\widehat{\ }, \breve{\ })$*-expressible.*

PROOF. Let $B = \{0, 1, b_1, b_2, \dots, b_{n-2}\}$, and let the permutation $\widehat{\ }$ be given by

$$(2\cdot3)\qquad \widehat{\ }\,;\ \text{def}:\ (0, 1)(b_1, b_2, \dots, b_{n-2}),\ (\text{i. e.}, 0\widehat{\ } = 1, 1\widehat{\ } = 0, b_1\widehat{\ } = b_2, \dots, b_{n-2}\widehat{\ } = b_1).$$

Now, for any $r = b_i \in B \setminus B^*$, $i = 1, \dots, n = 2$, there is exactly one integer j, $1 \leq j \leq n - 2$, such that $b_i^{\widehat{\ }j} = b$. Therefore $\delta_b(b_i^{\widehat{\ }j}) = 1$, while for all other positive integers t, $\delta_b(b_i^{\widehat{\ }t}) = 0$ $(1 \leq t \leq n - 2)$. Thus (2.1) becomes

$$\varrho_b(b_i) = (b_i\widehat{\ } \times 0) \times_{\frown} \dots \times_{\frown} (b \times 1) \times_{\frown} (0) = b,$$

since (see *Notation* 1.1) $a \times_{\frown} 0 = 0 \times_{\frown} a = a$. This proves (i).

To prove (ii), let $f(\xi)$ denote the right member of (2.2). Now $f(1) = 1^2(0\widehat{\ }) = 1$ since $\delta_b(1\widehat{\ }k) = 0$ for all $k = 1, 2, \dots, n = 2$. (See (2.3)). Moreover, $f(0) = 0$. Also, $f(b_i) = b_i^2(1)\widehat{\ } = 0$, since for exactly one integer j, $0 < j \leq n - 2$, $b_i^{\widehat{\ }j} = b$ (since $b \notin B^* (= \{0, 1\})$) and $\delta_b(b) = 1$. Thus $f(\xi) = \delta_1(\xi)$ as desired.

Finally, (iii) follows readily from the definition of $\delta_a(\xi)$.

The following corollary is extremely useful for our purposes.

COROLLARY 2.1. *Suppose* $(B, \times)$ *is a finite binary algebra which has exactly* n *elements,* $n \geq 3$, *and suppose* $(B^*, \times)$ *is a subalgebra of* $(B, \times)$ *where* $B^* = \{0, 1\}$. *Suppose* $\hat{}$ *is a permutation of* B *(with inverse* $\check{}$*) as given in* (2.3). *If for some* $b \in B \setminus B^*$ *the characteristic function* $\delta_b(\xi)$ *is* $(\times, \hat{}, \check{})$*-expressible, then* $(B, \times, \hat{})$ *is a regular subprimal algebra with* $(B^*, \times, \hat{})$ *as its core.*

PROOF. All the conditions (i)-(v) of Lemma 1.2 are readily verified, upon using Theorem 2.1 and Definition 2.1. Indeed, since $\delta_b(\xi)$ is expressible in terms of $\times, \hat{}, \check{}$, the same is true for $\delta_b(\xi\hat{})$, $\delta_b(\xi\hat{}^2), \ldots$. Similarly, since $\delta_1(\xi)$ is expressible (see (2.2) and (2.3)), therefore $\delta_1(\xi\hat{})\,(= \delta_0(\xi))$ is also expressible (in terms of $\times, \hat{}, \check{}$). Hence $\delta_a(\xi)$ is $(\times, \hat{}, \check{})$-expressible for all $a \in B$. Finally, since B is *finite*, we can express $\xi\check{}$ in terms of $\xi\hat{}$, and thus drop $\xi\check{}$ as a primitive operation. This proves the corollary.

We now introduce the following

DEFINITION 2.2. A *z-algebra* is a finite binary algebra $(B, \times)$ which is associative and such that

(1) for some $z \in B$, $z \neq 1$, z^{-1} is also in B,

(2) for some $\eta \in B$, $\eta \neq 0$, η is nilpotent.

We further agree that z, once chosen, is assumed to be fixed.

It is easily seen that the only four-element z-algebra is B given by

(2.4) $\qquad B = \{0, 1, \eta, z\}$; η nilpotent; z has an inverse in B.

Moreover, since $\eta^2 = \eta$ implies $\eta = 0$, we must have $\eta^2 = 0$. Similarly, since $z^2 = z$ implies $z = 1$, we must have $z^2 = 1$. Hence

(2.5) $\qquad (B, \times) \cong (I/(4), \times)$ (= semi-group of integers, mod 4).

Now, define $\hat{}$ by

(2.6) $\qquad \hat{}$: def: $(0, 1, \eta)(z)$ (i. e., $0\hat{} = 1, 1\hat{} = \eta, \eta\hat{} = 0, z\hat{} = z$).

It is readily verified that

$$\delta_z(\xi) = (\xi\xi\hat{})^2;\ \delta_1(\xi) = \xi^2\left(\delta_z(\xi) \times_{\_} \delta_z(\xi\hat{})\right)\hat{};\ \delta_0(\xi) = \delta_1(\xi\hat{});$$

(2.7)

$$\delta_\eta(\xi) = \delta_1(\xi\hat{}^2);\ \delta_0(\xi)\,\delta_1(\xi) = 0;\ [\delta_0(\xi)\,\delta_1(\xi)]\hat{} = 1;\ \varrho_z(\xi) = \xi.$$

Hence, by Lemma 1.2, $(B, \times, \hat{})$ is a regular subprimal algebra with $(B^*, \times, \hat{})$ as core, where $B^* = \{0, 1, \eta\}$.

Since a z-algebra B is finite, it readily follows that $z^\lambda = z^\mu$, for some integers λ, μ, $\lambda > \mu$. Since, moreover, B is associative, therefore $z^{\lambda-\mu} = 1$, $\lambda - \mu > 0$. In view of this, we may (and shall) adopt the following

NOTATION 2.1. The integer m will always denote the least positive integer such that

(2.8) $z^m = 1$, and $\gamma^m = 0$ for *every* nilpotent element γ in B.

REMARK 2.1. Since we have already shown that the (one and only) four-element z-algebra $(B, \times)$, endowed with the permutation $\frown$ given in (2.6), yields a semi-primal algebra $(B, \times, \frown)$, we shall assume from now on that B has at least five elements.

Let $(B, \times)$ be a z-algebra. A *proper element* of B is any element u of B such that $u \neq 0$, $u \neq 1$, $u \neq z$. For any positive integer k, a *proper-k-product* (pr.-k-pdt.) is any product consisting of k — *th* powers of proper elements of B. The *length* of a proper-k-product is the number of *distinct* proper elements appearing as factors. B is said to have *rank* r if r is the greatest integer such that B has a proper-m-product $P(a_1^m, \ldots, a_r^m)$ of legth r, where m is as in *Notation* 2.1, and where $P(a_1^m, \ldots, a_r^m)$ is not nilpotent. In other words,

(2.9) B has *rank* r if there exists a pr.-m-pdt. $P(a_1^m, \ldots, a_r^m)$ of length r such that $P(a_1^m, \ldots, a_r^m)$ is *not* nilpotent, while every pr.-m-pdt. of length greater than r is nilpotent-Here $P(a_1^m, \ldots, a_r^m)$ denotes the product of $a_1^m, \ldots, a_r^m$ *in some order* (which need *not* be the ordering $a_1^m, \ldots, a_r^m$), where $a_1, \ldots, a_r$ are *distinct* and *proper*.

We also agree that

(2.10) B has *rank zero* if a^m is nilpotent for every proper element a of B (and hence $a^m = 0$; see *Notation* 2.1).

Clearly, in any z-algebra B consisting of n elements, every pr.-m-pdt. of length $n - 3$ must contain a zero factor, since B has at least one nilpotent proper element. Hence

(2.11) $0 \leq r < n - 3$, ($r =$ rank of the z-algebra B).

Next, suppose the z-algebra B has rank r, and suppose (see (2.9)) $P(a_1^m, \ldots, a_r^m)$ is not nilpotent (all a_i's proper and distinct). We clain that

(2.12) If $r > 0$ and $[P(a_1^m, \ldots, a_r^m)]^m = \beta$, then $\beta = a_i$ for some $i = 1, \ldots, r$, or β is not a proper element.

For suppose β were a proper element, and suppose $\beta \neq a_i (i = 1, \dots, r)$. Now consider

$$[P(a_1^m, \dots, a_r^m)]^n \times (\beta^m) = \beta^{m+1}. \tag{2.13}$$

The left-side of (2.13) is of length $r + 1$ and hence must be nilpotent (see (2.9)). Therefore β^{m+1} (and hence β) is nilpotent. Thus $P(a_1^m, \dots, a_r^m)$ is nilpotent, a contradiction. This proves (2.12).

We are now in a position to state the following

THEOREM 2.2 (Principal Theorem). *Suppose* $(B, \times)$ *is a z-algebra. Then there exists a permutation* $\widehat{\ }$ *of* B *such that* $(B, \times, \widehat{\ })$ *is a regular subprimal algebra (of species* (2,1)).

PROOF. First, if B has rank zero, then (see (2.10)), $a^m = 0$ for every proper element a of B. Now define $\widehat{\ }$ by,

$$\widehat{\ }: \text{def}: (0, 1)(z, a_1, a_2, \dots, a_{n-3}),\ (a_1, \dots, a_{n-3} \text{ are the proper elements of } B \text{ ordered in an arbitrary way}). \tag{2.14}$$

It is readily verified that (see *Notation* 2.1 and *Remark* 2.1)

$$\delta_z(\xi) = [[[\xi^m \times (\xi\widehat{\ })]\widehat{\ }]^n]\widehat{\ }. \tag{2.15}$$

Hence, by Corollary 2.1, $(B, \times, \widehat{\ })$ is a regular subprimal algebra.

Next, consider the case where $r \geq 1$ ($r =$ rank of B). In view of (2.9), we know that one of the following eventualities must occur:

Case 1: There exists some pr.-m-pdt. of length r, say $P(a_1^m, \dots, a_r^m)$, which is not nilpotent and such that

$$\beta = \text{def} = [P(a_1^m, \dots, a_r^m)]^n,\ \beta \neq a_i\ (i = 1, \dots, r),\ \beta \text{ not nilpotent},\ r \geq 1. \tag{2.16}$$

Case 2: For *every* pr.-m-pdt. $P(a_1^m, \dots, a_r^m)$ of length r which is not nilpotent, $\beta = a_i$ for some $i = 1, \dots, r$, where $\beta = [P(a_1^m, \dots, a_r^m)]^m$.

From now on we let η be a *nonzero* nilpotent element of B (see Definition 2.1). Observe that η is distinct from each a_i in (2.16), since β is not nilpotent.

First, let us consider *Case* 1. In *Case* 1, we know that by (2.12), β is *not* proper and hence $\beta = 1$ or $\beta = z$ (observe that $\beta \neq 0$ by (2.16)). For

either value of β, we define $\widehat{\ }$ by

$$\widehat{\ }: \text{def}: (0, 1)(z, a_1, \ldots, a_r, \ldots, \eta).$$

It is easily checked that

$$\delta_z(\xi) = [(\xi^m) P((\xi\widehat{\ })^m, (\xi\widehat{\ }^2)^m, \ldots, (\xi\widehat{\ }^r)^m)]^{m^2}. \tag{2.17}$$

In verifying (2.17), observe that for $\xi = z$ (2.17) reduces to $\delta_z(z) = \beta^m = 1$, since $z^m = 1$. Moreover, if ξ is proper, the expression in square brackets in the right-side of (2.17) is either a pr.-m-pdt. of length $r+1$ (and hence is nilpotent), or this expression contains $\eta^m (= 0)$ as a factor. In either case, (2.17) follows readily. Finally, (2.17) is trivially verified for $\xi = 0$ or $\xi = 1$. Now, a combination of (2.17) and Corollary 2.1 shows that $(B, \times, \widehat{\ })$ is a regular subprimal algebra in this case.

Next, consider *Case* 2. We distinguish two subcases.

Case 2A: rank of $B = r > 1$. In this case, let $P(a_1^m, \ldots, a_r^m)$ be a pr.-m-pdt. of length r. By hypothesis,

$$\beta = [P(a_1^m, \ldots, a_r^m)]^m = a_i \quad \text{for some } i = 1, \ldots, r. \tag{2.18}$$

Now, define a permutation $\widehat{\ }$ of B by

$$\widehat{\ }: (0, 1)(z, a_1, a_i, a_3, a_4, \ldots, a_{i-1}, a_2, a_{i+1}, a_{i+2}, \ldots, a_r, \ldots, \eta). \tag{2.19}$$

In other words, the effect of $\widehat{\ }$ on the a_j's is that we interchange the positions of a_2 and a_i, but leave all the other a_j's in their natural ordering. For example, if $i = 1$ then above effect becomes $(z, a_2, a_1, \ldots)$ while if $i=2$, above effect becomes $(z, a_1, a_2, \ldots)$ (i. e., the a_j's are now in their natural ordering). It is readily verified that

$$\delta_z(\xi) = [[[(\xi^m) P((\xi\widehat{\ })^m, (\xi\widehat{\ }^i)^m, (\xi\widehat{\ }^3)^m, \ldots, (\xi\widehat{\ }^{i-1})^m, (\xi\widehat{\ }^2)^m, (\xi\widehat{\ }^{i+1})^m, \ldots, (\xi\widehat{\ }^r)^m)]^m]\widehat{\ }^2]^m. \tag{2.20}$$

In verifying (2.20), observe that $\delta_z(z) = (((P(a_1^m, a_2^m, \ldots, a_r^m))^m)\widehat{\ }^2)^m = (a_i\widehat{\ }^2)^m = z^m = 1$. The verification of (2.20) for all other values of ξ is similar to the verification of (2.17). Hence, by (2.20) and Corollary 2.1, $(B, \times, \widehat{\ })$ is a regular subprimal algebra (in *Case* 2A).

Case 2B: rank of $B = r = 1$. First, if B has at least two distinct nonzero nilpotent elements η, η', say, we define $\widehat{\ }$ by

$$\widehat{\ }: (0, 1)(z, a_1, \eta, \ldots, \eta'). \tag{2.21}$$

Here a_1 is determined as follows: Since the rank of B is equal to 1, there therefore exists a proper element a_1, say, such that $(a_1^m)^m = \beta = a_1$, i. e., $a_1^{m^2} = a_1$ (see (2.18)). Now, it is readily verified that

$$\delta_z(\xi) = [[[[{}'\xi^m)(\xi^{\frown})^m]^m]^{\frown}]^m]^{\frown}. \tag{2.22}$$

Hence, by (2.22) and Corollary 2.1, $(B, \times, {}^{\frown})$ is a regular subprimal algebra in this last case also. There remains only the following case:

(2.23) rank of $B = r = 1$; (2.18) holds (with $r = 1$); η is the only nonzero nilpotent element of B.

Now, since η^2 is nilpotent, we must have $\eta^2 = 0$ (otherwise, $\eta^2 = \eta$ and hence $\eta = 0$, contradiction). Let

$$B = \{0, 1, z, \eta, a_1, \ldots, a_{n-4}\}. \tag{2.24}$$

Moreover, since we are still in *Case* 2, we know that *every* pr.-m-pdt. of length 1 ($r = 1$) satisfies: $(a_k^m)^m = \beta = a_k$, and hence $a_k^{m^2} = a_k$ for each $k = 1, \ldots, n-4$. We claim that

(2.25) $a_k^m = a_k$, and $a_t \times a_k$ is nilpotent, for all $k = 1, \ldots, n-4$, and all $t = 1, \ldots, n-4$, $t \neq k$.

We prove (2.25) by contradiction. Thus suppose $a_i^m \neq a_i$ for some i. Clearly, a_i^m is not nilpotent (see (2.23), (2.24)). Moreover, if $a_i^m = z$, then $a_i = (a_i^m)^m = z^m = 1$, a contradiction. Hence $a_i^m \neq z$. Similarly $a_i^m \neq 1$. Therefore $a_i^m = a_j$ for some j. If $j \neq i$, then $a_i^{m^2+m} = a_j^m a_i^m$ is nilpotent since $r = 1$, and this forces a_i to be nilpotent, a contradiction. Hence, $a_k^m = a_k$ for every $k = 1, \ldots, n-4$. Finally, if $t \neq k$, then $a_t \times a_k$ is nillpotent (since $a_t a_k = a_t^m a_k^m$ and $r = 1$). This proves (2.25).

Now, if $a_k \eta = z$ then $z\eta = a_k \eta^2 = 0$, and hence $\eta = z^{-1} \cdot 0 = 0$, a contradiction. Therefore, $a_k \eta \neq z$ for any $k = 1, \ldots, n-4$. Similarly $\eta a_k \neq z$ for any k. Moreover, if $a_k^2 = z$, then $a_k^{2m} = z^m = 1$ and hence $z = a_k^2 = (a_k^m)^2 = 1$, a contradiction. Therefore $a_k^2 \neq z$, $k = 1, \ldots, n-4$. We have thus shown that

(2.26) $(B^*, \times)$ is a subalgebra of $(B, \times)$ where $B^* = B \setminus \{z\}$.

Now, define ${}^{\frown}$ by

$${}^{\frown}: \text{def}: (0, 1, a_1, \ldots, a_{n-4}, \eta)(z). \tag{2.27}$$

Clearly, z is ex-expressible by $\varrho_z(\xi) = \xi$. Moreover,

$$\delta_z(\xi) = [\xi^m \prec (\xi^{\frown})^m \prec (\xi^{\frown 2})^m]^m, \tag{2.28}$$

$$\delta_1(\xi) = [[[\xi^m (\xi^{\frown})^m]^m]^{\smile}]^m. \tag{2.29}$$

Hence, $\delta_1(\xi^{\frown})$, $\delta_1(\xi^{\frown 2})$, ... are all expressible (in terms of $\prec, {}^{\frown}, {}^{\smile}$), and thus $\delta_a(\xi)$ is expressible for every $a \in B$. Moreover,

$$\delta_0(\xi)\,\delta_1(\xi) = 0, \qquad (\delta_0(\xi)\,\delta_1(\xi))^{\frown} = 1. \tag{2.30}$$

Hence, by Lemma 1.2, $(B, \times, {}^{\frown}, {}^{\smile})$ is a regular subprimal algebra. Since B is *finite*, we can always express $\xi^{\smile}$ in terms of $\xi^{\frown}$ and hence we may delete $\xi^{\smile}$ as a primitive operation. Thus $(B, \times, {}^{\frown})$ is a regular subprimal algebra (with $(B^*, \times, {}^{\frown})$ as its core). This completes the proof.

3. Applications.

In this section we apply Theorem 2.2 to certain classes of rings. Consider for a moment a finite ring R with identity 1, where R is *not* commutative. A well-known result of Herstein [3] asserts that such a ring R does indeed possess a *nonzero* nilpotent element η. But then $z = 1 + \eta$ certainly has an inverse in R, since if $\eta^k = 0$, then $(1+\eta)(1 - \eta + \ldots \mp \eta^{k-1}) = 1 \mp \eta^k = 1$; and, of course, $z \neq 1$. Thus $(R, \times)$ is a z-algebra. Applying Theorem 2.2, we now obtain

THEOREM 3.1. *Let $(R, +, \prec)$ be any finite ring which is not commutative (or R has a nonzero nilpotent element) and which has an identity. Then there exists a permutation ${}^{\frown}$ of R such that $(R, \times, {}^{\frown})$ is a regular subprimal algebra. In particular, the complete matrix ring $M_n(F)$ over a field F $(n>1)$ always possesses a permutation ${}^{\frown}$ such that $(M_n(F), \times, {}^{\frown})$ is a regular subprimal algebra.*

An immediate consequence of this theorem is the following

COROLLARY 3.1. *Let $(R, +, \times)$ be any finite ring with identity. If $(R, \times, {}^{\frown})$ is never semi-primal for any permutation ${}^{\frown}$ of R, then R is commutative.*

Now, suppose that R is *any* finite ring with identity 1. If R happens to have a *nonzero* nilpotent element η, then as we have just seen, $(R, \times)$ is a z-algebra (with $z = 1+\eta$), and Theorem 2.2 now guarantees the existence of a permutation ${}^{\frown}$ of R such that $(R, \prec, {}^{\frown})$ is a regular subprimal algebra.

Hence we may (and shall) assume that R has *no* nonzero nilpotent elements, and therefore R is commutative, by Herstein's Theorem [3]. Thus R is a finite commutative ring with identity and with zero radical, and hence [4]

$$R \cong GF(n_1) \oplus \ldots \oplus GF(n_t); \quad 2 \leq n_1 \leq \ldots \leq n_t, \tag{3.1}$$

i. e., R is isomorphic to the complete direct sum of fields $GF(n_i)$, $n_i = p_i^{k_i}$ (p_i prime), $i = 1, \ldots, t$. *From now on we assume that R is of characteristic different from* 2 *and with at least three elements. Let*

$$R = \{0, 1, -1, \gamma_1, \ldots, \gamma_{n-3}\}. \tag{3.2}$$

We proceed to define a permutation $\widehat{\ }$ of R. This we do in several stages depending on the values of t and n_i in (3.1).

Case 1: If $t = 1$, define $\widehat{\ }$ by

$$\widehat{\ }: (0,1)(\gamma_1, \ldots, \gamma_{n-3}, -1) \text{ (i.e., } 0\widehat{\ } = 1, 1\widehat{\ } = 0, \gamma_1\widehat{\ } = \gamma_2, \ldots, (-1)\widehat{\ } = \gamma_1). \tag{3.3}$$

Case 2: If $t > 2$. Via the direct sum representation (3.1) of R, we now let $\{1, -1, \alpha_1, \ldots, \alpha_\sigma\}$ be the set of all elements of R whose $t-th$ components (in (3.1)) are different from zero, and choose the notation such that

$$\alpha_1 = (0, 1, 1, \ldots, 1), \qquad \alpha_2 = 1(-1)\alpha_1 \ldots \alpha_\sigma. \tag{3.4}$$

Observe that, since one of the α_i's is $(0, 0, \ldots, 0, 1)$, therefore $\alpha_2 = (0, 0, \ldots, 0, z_t)$, $z_t \neq 0$, $z_t \in GF(n_t)$. Let $\{\beta_1, \ldots, \beta_\tau\}$ be all the remaining element of $R(\neq 0)$. Now, define $\widehat{\ }$ by

$$\widehat{\ }: (0,1)(\beta_1, \ldots, \beta_\tau, \alpha_\sigma, \alpha_{\sigma-1}, \ldots, \alpha_2, \alpha_1, -1), \ (1(-1)\alpha_1 \ldots \alpha_\sigma = \alpha_2), \tag{3.5}$$

and where the only condition we impose on the β_i's is

$$\beta_1 = (1, 0, 0, \ldots, 0), \qquad \beta_2 = (0, 1, 0, 0, \ldots, 0), \qquad (t \geq 3). \tag{3.6}$$

Case 3: If $t = 2$ and $n_1 = n_2 (= n_t)$. In this case, $n_1 > 2$ (since the characteristic of R is not 2). Let $\{1, -1, \alpha_1, \ldots, \alpha_\sigma\}$ be as in case 2 above but choose the notation now such that

$$\alpha_1 = (1, \xi), (\xi \neq 0, \xi \neq 1), \quad \text{and } \alpha_2 = 1(-1)\alpha_1 \ldots \alpha_\sigma. \tag{3.7}$$

Define $\widehat{\ }$ now as in (3.5) and (3.7) (but no restriction on β_1, β_2).

Case 4: If $t = 2$ and $n_1 < n_2 (= n_t)$. In this case, define $\frown$ as in (3.5) (but no restriction on $\beta_1, \beta_2, \alpha_1$).

Arguments parallel to those given in [6; Theorems 4,5] show that the following formulas hold in the designated cases. We omit the details.

$$\delta_{-1}(\xi) = (((\xi^{\smile} \xi^{\smile 2} \dots \xi^{\smile n-3})^{\frown})^{n-1})^{\frown} \quad \text{(in } \textit{Case } 1, \text{ if } n > 3)$$

$$\delta_{-1}(\xi) = \xi\xi^{\smile} \quad \text{(in } \textit{Case } 1, \text{ if } n = 3)$$

$$\delta_{-1}(\xi) = ((\xi\xi^{\smile} \xi^{\smile 2} \dots \xi^{\smile n})^{\frown 2})^2 \quad \text{(in } \textit{Case } 2, \textit{Case } 3, \textit{Case } 4).$$

Hence, by Corollary 2.1, $(R, \curlywedge, \frown)$ is a regular subprimal algebra (with $(\{0, 1\}, \times, \frown)$ as core). A combination of this and Theorem 3.1 yelds the following

THEOREM 3.2. *Let $(R, +, \times)$ be any finite (not necessarily commutative) ring with identity but of characteristic different from two. Then there exists a permutation $\frown$ of R such that $(R, \times, \frown)$ is a regular subprimal algebra.*

In conclusion, we remark that a ring R of characteristic two need *not* possess a permutation $\frown$ for which $(R, \times, \frown)$ is a regular subprimal algebra. For example $(GF(2^2), +, \times)$ cannot be converted to a regular subprimal algebra $(GF(2^2), \times, \frown)$. This follows from Lemma 1.1 (ii), (iii). Similar remark can be made in regard to $GF(2) \oplus \dots \oplus GF(2)$. We omit the details.

Brigham Young University
Provo, Utah
and
University of California
Santa Barbara, California

REFERENCES

[1] A. L. FOSTER, *An existence theorem for functionally complete universal algebras*, Math. Z. 71 (1959), 69-82.

[2] A. L. FOSTER and A. F. PIXLEY, *Semi-categorical algebras I, semi-primal algebras*, Math Z. 83 (1964), 147-169.

[3] I. N. HERSTEIN, *A note on rings with central nilpotent elements*, Proc. Amer. Math. Soc 5 (1954), 620.

[4] N. H. MCCOY, *Rings and Ideals*, Carus Math. Monog. 8, Buffalo, N. Y.: Math. Assoc Amer., 1947.

[5] A. YAQUB, *Semi-primal categorical independent algebras*, Math. Z. 93 (1966), 395-403.

[6] A. YAQUB, *On certain classes of — and an existence theorem for — primal clusters*, Ann Scuola Norm. Sup. Pisa 20 (1966), 1-13.