PACIFIC JOURNAL OF MATHEMATICS
Vol. 74, No. 2, 1978

EQUATIONAL DEFINABILITY OF ADDITION IN CERTAIN RINGS

HAL G. MOORE AND ADIL YAQUB

Boolean rings and Boolean algebras, though historically and conceptually different, were shown by Stone to be *equationally* interdefinable. Indeed, in a Boolean ring, addition can be defined in terms of the ring multiplication and the successor operation (Boolean complementation) $x^\wedge = 1 + x(=1 - x)$. In this paper, it is shown that this type of equational definability of addition also holds in a much wider class of rings, namely periodic rings (ring satisfying $x^m = x^n$, $m \neq n$) in which the idempotent elements are "well behaved." More generally, the following theorem is proved:

Suppose R is a ring with unity 1, not necessarily commutative. Suppose further that R satisfies the identity $x^n = x^{n+1}f(x)$ where n is a fixed positive integer and $f(x)$ is a fixed polynomial with integer coefficients. If, further, the idempotent elements of R commute with each other, then addition in R is equationally definable in terms of multiplication in R and the successor operation $x^\wedge = 1 + x$.

Some new classes of rings to which this theorem applies are exhibited.

1. The periodic case. In this section, we shall consider a periodic ring R with unity 1 in which the idempotent elements commute with each other, and will give a *direct* proof of the equational definability of the "$+$" of R in terms of "$\times$" and the successor operation $x^\wedge$. This direct proof avoids the axiom of choice. We begin with a formal definition of a *periodic* ring.

DEFINITION 1. A ring R is called *periodic* if there exist fixed integers m and n with $m > n \geqq 1$ such that for all x in R, $x^n = x^m$.

LEMMA 1. *Let R be a periodic ring with unity* 1. *Then* (i) *For each x in R, $x^{(m-n)n}$ is idempotent.* (ii) *x is nilpotent if, and only if $x^n = 0$.*

Proof. (i) It can be shown by induction that the identity $x^n = x^m$ $(m > n \geqq 1)$ implies that for all positive integers r

$$x^n = x^{n+r}(x^{m-n-1})^r . \tag{1}$$

In particular $x^n = x^{2n}(x^{m-n-1})^n$. Let $e = (x^{m-n})^n$. It is readily verified that $e^2 = e$, which proves (i). Part (ii) follows at once from equation (1).

LEMMA 2. *Let R be a ring with unity 1 in which all of the idempotent elements commute with each other. Then all the idempotent elements of R lie in the center of R.*

Proof. Let $e^2 = e \in R$. It is readily verified that for each $x \in R$, $e + ex - exe$ is idempotent and hence $e(e + ex - exe) = (e + ex - exe)e$. Thus, $ex = exe$. Similarly $xe = exe$ and so $ex = xe$ proving the lemma.

To aid in our proof of the main theorem, we introduce some notation. Let $(R, +, \times)$ be *any* (not necessarily periodic) ring with unity 1. Let $x \in R$. We define the (unary) successor operation $x^\wedge$ in R by

$$x^\wedge = x + 1 \tag{2}$$

with an inverse successor operation $x^\vee$ given by

$$x^\vee = x - 1 . \tag{3}$$

We also use following notation:

$$x^{\wedge k} = (\cdots((x^\wedge)^\wedge)^\wedge \cdots)^\wedge , \quad (k\text{-iterations}), \tag{4}$$

with a similar definition for $x^{\vee k}$. Moreover for all $a, b \in R$ we define the (binary) operation

$$a \times_\wedge b = (a^\wedge \times b^\wedge)^\vee \quad (= a + b + ab) . \tag{5}$$

It is readily verified that for all $a \in R$,

$$a \times_\wedge 0 = 0 \times_\wedge a = a . \tag{6}$$

We are now in a position to give a direct proof of

THEOREM 1. *Let R be a periodic ring with unity 1 which satisfies the identity $x^m = x^n$, $m > n \geqq 1$. Suppose that all the idempotent elements of R commute with each other. Then the "$+$" of R is equationally definable in terms of the "$\times$" of R and the successor operation $^\wedge$. Indeed for all $x, y \in R$ we have*

$$\begin{cases} x + y = [x(x^{m-n-1}y)^\wedge(x^{(m-n)n})] \times_\wedge \\ \qquad [x^\wedge((x^\wedge)^{m-n-1}y^\vee)^\wedge((x^{(m-n)n})^\vee)^2] . \end{cases} \tag{7}$$

Here, $x^\vee = x^{\wedge q-1}$ where $q = 2^m - 2^n$ and $x \times_\wedge y = (x^\wedge \times y^\wedge)^{\wedge q-1}$.

Proof. Let x_0, y_0 be arbitrary but fixed elements of R, and let

$$e = x_0^{(m-n)n} . \tag{8}$$

Then, by Lemmas 1, 2, e is a *central* idempotent element of R. Let

$$(9) \qquad \mathrm{Re} = \{re \mid r \in R\}\,; \quad R(1-e) = \{r(1-e) \mid r \in R\}\,.$$

The mapping

$$(10) \quad \sigma\colon R \longrightarrow \mathrm{Re} \oplus R(1-e)\,; \quad \sigma(r) = (re,\, r(1-e))\,, \quad (r \in R)\,,$$

is readily seen to be an onto isomorphism:

$$(11) \qquad \sigma\colon R \cong \mathrm{Re} \oplus R(1-e)\,, \quad (\sigma \text{ is onto}).$$

Moreover, by (10),

$$(12) \qquad \sigma(x_0) = (x_0e,\, x_0(1-e))\,; \quad \sigma(y_0) = (y_0e,\, y_0(1-e))\,.$$

Now, since the operations in $\mathrm{Re} \oplus R(1-e)[=R]$ are componentwise, it suffices to verify (7) for *both* of the following substitutions [see (11), (12)]:

(i) $x = x_0e$, $y = y_0e$;

(ii) $x = x_0(1-e)$, $y = y_0(1-e)$.

Verification of (7) *when* (i) *holds*:

In this case, x_0e is a *unit* in Re, since by (8) and the fact that e is a *central* idempotent,

$$(x_0e)^{(m-n)n-1}(x_0e) = (x_0e)(x_0e)^{(m-n)n-1} = ee\,.$$

Moreover, since $(x_0e)^m = (x_0e)^n$ and x_0e is a unit in Re, we have

$$(13) \qquad (x_0e)^{m-n} = ee = e[=\text{identity of Re}]\,.$$

Hence the right side of (7), with $x = x_0e$, $y = y_0e$, reduces to [see (13)]

$$(14) \qquad [x_0e(e + (x_0e)^{m-n-1}(y_0e))] \mathbin{\text{✕}_{\wedge}} 0$$

because $(((x_0e)^{(m-n)n})^{\smile})^2 = (e^{\smile})^2 = (e-e)^2 = 0$. Now, by (6) and (13), (14) reduces to

$$x_0e + (x_0e)^{m-n}(y_0e) = x_0e + y_0e = x + y\,,$$

which verifies (7) in this case.

Verification of (7) *when* (ii) *holds*:

To begin with, observe that $1-e$ is an idempotent element which is in the *center* of R, and in fact $1-e$ is the unity element of $R(1-e)$. Hence

$$(15) \quad x^{(m-n)n} = [x_0(1-e)]^{(m-n)n} = x_0^{(m-n)n}(1-e) = e(1-e) = 0\,,$$

using (8). Thus $x = x_0(1-e)$ is a *nilpotent* element of $R(1-e)$, and hence (see [3; p. 8])

(16) $x^{\wedge} = (1 - e) + x_0(1 - e)$ is a *unit* in $R(1 - e)$.

Therefore, as in the above proof [see (13)],

(17) $$\begin{aligned}(x^{\wedge})^{m-n} &= [(1 - e) + x_0(1 - e)]^{m-n} \\ &= 1 - e[=\text{identity element of } R(1 - e)] .\end{aligned}$$

Hence the right side of (7), with $x = x_0(1 - e)$, $y = y_0(1 - e)$, reduces to [see (15)]

(18) $$0 \times_{\wedge} [x^{\wedge}((1 - e) + (x^{\wedge})^{m-n-1}y^{\vee})(0^{\vee})^2] .$$

By (6), (16), (17), (3), the expression in (18) reduces to

$$x^{\wedge} + (x^{\wedge})^{m-n}y^{\vee} = x^{\wedge} + y^{\vee} = x + y ,$$

and again (7) is verified. Thus (7) is an identity of the ground ring R.

Now, since $x^n = x^m$ holds in R, in particular $(2^m - 2^n) \cdot 1 = 0$. Let $q = 2^m - 2^n$. Then $x^{\wedge q} = x$ in R and thus $x^{\vee} = x^{\wedge q-1}$. Therefore (5) implies that $x \times_{\wedge} y = (x^{\wedge} \times y^{\wedge})^{\wedge q-1}$ and the "+" of R is indeed equationally definable via (7) and these remarks in terms of the "$\times$" of R and $\wedge$ only. This proves the theorem.

REMARK. Since a Boolean ring R with identity has characteristic 2, $x^{\wedge} = x^{\vee} = x^*$ is the Boolean complement [5]. Also, a Boolean ring is *periodic* (satisfying $x = x^2$) and *commutative* [5]. Therefore R satisfies all of the hypotheses of Theorem 1. Moreover, (7) now reduces to (since $m = 2$, $n = 1$)

$$x + y = [xy^{\wedge}x] \times_{\wedge} [x^{\wedge}(y^{\vee})^{\wedge}(x^{\vee})^2] = xy^{\wedge} \times_{\wedge} x^{\wedge}y$$

which becomes, using the definition of union [5] in a Boolean algebra,

$$x + y = xy^* \cup x^*y .$$

This is the familiar definition of addition in the Boolean case [5]. Therefore (7) may be viewed as a generalization to periodic rings of the formula for addition in the Boolean situation.

At the end of this paper we give some examples of rings, some commutative and some not commutative, for which Theorem 1 applies.

2. The general case.

We now proceed to extend the results of the previous section to a class of rings satisfying certain types of polynomial identities. We begin with the following

DEFINITION 2. A (not necessarily commutative) ring R is called a *local* ring if each x in R is either nilpotent or else invertible in

R. We are now prepared to prove the following

LEMMA 3. *Let R be a ring with unity* 1, *and let n be a fixed positive integer. Suppose that $f(t)$ is a fixed polynomial with integer coefficients, and that, for all $x \in R$,*

$$x^n = x^{n+1}f(x) . \tag{19}$$

If, further, all the idempotent elements of R commute with each other, then R is isomorphic to a subdirect sum of local rings R_i $(i \in \Gamma)$.

Proof. An easy induction, which we omit, shows that equation (19) implies

$$x^n = x^{n+r}[f(x)]^r \quad \text{for all positive integers } r. \tag{20}$$

In particular $x^n = x^{2n}[f(x)]^n$. Let $e = x^n[f(x)]^n$. Then $e^2 = e$. Hence, by Lemma 2, we have the following:

(21) If $x \in R$, then $e = x^n\{f(x)\}^n$ is a *central* idempotent.

We recall, by Birkhoff's theorem [1], that R is isomorphic to a subdirect sum of subdirectly irreducible rings R_i $(i \in \Gamma)$. We claim that each R_i is a local ring. To prove this, let $\sigma_i: R \to R_i$ be the natural homomorphism of R onto R_i. For $\bar{x} \in R_i$ let $x \in R$ be any preimage under σ_i. Let $e = x^n\{f(x)\}^n$. Then by (21), e is a central idempotent in R. Let $\bar{e} = \sigma_i(e)$. Then $\bar{e}$ is an idempotent in the center of R_i. Now let

$$I_1 = \{\bar{e}\bar{r} \mid \bar{r} \in R_i\}; \quad I_2 = \{\bar{r} - \bar{e}\bar{r} \mid \bar{r} \in R_i\} .$$

Since $\bar{e}$ is in the center of R_i, both I_1 and I_2 are ideals in R_i. Moreover $I_1 \cap I_2 = (\bar{0})$. But R_i is subdirectly irreducible which forces either I_1 or I_2 to be $(\bar{0})$. If $I_1 = (\bar{0})$, $\bar{e} = \bar{e}^2 = \bar{0}$, hence $\bar{e} = \bar{0}$. If $I_2 = (\bar{0})$, then $\bar{e} = \bar{1}$. Since $\bar{e} = (\bar{x})^n\{f(\bar{x})\}^n$, we have shown that

(22) If $\bar{x} \in R_i$, then $(\bar{x})^n\{f(\bar{x})\}^n = \bar{0}$ or $(\bar{x})^n\{f(\bar{x})\}^n = \bar{1}$.

Moreover, since R_i clearly satisfies (20), we conclude from (22) that

(23) If $\bar{x} \in R_i$, then $(\bar{x})^n = \bar{0}$ or $(\bar{x})^{-1} = (\bar{x})^{n-1}\{f(\bar{x})\}^n \in R_i$.

Hence R_i is a local ring, and the lemma is proved.

Next, we prove the following

LEMMA 4. *In the notation and under all the hypotheses of Lemma* 3, *the set N_i of nilpotent elements in the local ring R_i is*

an ideal in R_i and R_i/N_i is a field. Moreover, N_i coincides with the Jacobson radical J_i of R_i.

Proof. Suppose that $x \in J_i$. Then, as we proved in Lemma 3, $x^n\{f(x)\}^n$ is an idempotent element in J_i, and hence $x^n\{f(x)\}^n = 0$. Therefore, by (20), $x^n = 0$, and hence $J_i \subseteqq N_i$. Now, suppose that $a \in N_i$ and $x \in R_i$. Since R_i is a local ring, ax is either nilpotent or is a unit in R_i. It is easy to see that ax is *not* a unit in R_i (since a is nilpotent), and hence ax is nilpotent. Therefore, ax is right quasi-regular for all x in R_i, and hence $a \in J_i$. Thus, $N_i \subseteqq J_i$, and hence $N_i = J_i$. Now, observe that the identity $x^n = x^{n+1}f(x)$ is inherited by the division ring R_i/N_i and, moreover, both n and $f(x)$ are fixed. Hence, R_i/N_i is a field, and the lemma is proved.

LEMMA 5. *In the notation and under all the hypotheses of Lemmas 3 and 4, there exists a monic polynomial $g(x)$ with integer coeficients and an integer $m > 1$ such that for all x in R,*

$$x^m = x^{m+1}g(x) . \tag{24}$$

Proof. Let $x = 2$ in (19). This gives $2^n = 2^{n+1}f(2)$, and hence the characteristic of R is a positive integer q. Now let $p_1, p_2, \cdots, p_s$ be all the distinct *prime* factors of q. Let $x \in R_i$, $x \notin N_i$, and let $\sigma_i: R_i \longrightarrow R_i/N_i$ be the natural homomorphism of R_i onto the field R_i/N_i. Let $\sigma_i: x \longrightarrow \bar{x}$. Note that the field R_i/N_i has prime characteristic, and moreover the subring $\langle \bar{x} \rangle$ generated by $\bar{x}$ is a finite field; that is,

$$\langle \bar{x} \rangle = GF(p_j^{k_j}) \subseteqq R_i/N_i . \tag{25}$$

Moreover, since the characteristic of the field R_i/N_i must divide the characteristic q of R, it follows that the prime p_j is one of the prime factors of q. Also in view of (19) we have

$$(\bar{x})^n = (\bar{x})^{n+1}f(\bar{x})$$

for all $\bar{x} \in R_i/N_i$. We define the polynomial $h(t)$ of degree a by

$$h(t) = t^{n+1}f(t) - t^n .$$

Since $f(t)$ has integer coefficients, so does $h(t)$. From (25) we conclude that k_j is the degree of the irreducible (minimal) polynomial which $\bar{x}$ satisfies over $GF(p_j)$ and hence $k_j \leqq a$, where we now view $h(t)$ as a polynomial in $GF(p_j)[t]$. But then k_j divides $a!$ and, hence,

$$t^{p_j^{k_j}} - t \text{ divides } t^{p_j^{a!}} - t . \tag{26}$$

We can, therefore, conclude from (25) and (26) that

$$(\bar{x})^{p_j^{a_j}} - \bar{x} = \bar{0} \quad (=\text{the zero of } R_i/N_i) .$$

Therefore, for $x \in R_i$, $x^{p_j^{a_j}} - x$ is nilpotent in R_i. Since, moreover, R_i satisfies (20), we conclude that

$$(27) \qquad (x^{p_j^{a_j}} - x)^n = 0 \quad \text{for all} \quad x \in R_i .$$

(Note that if x is in N_i, then $x^n = 0$, from which (27) also follows.) Now define the monic polynomial $u(x)$ by

$$(28) \qquad u(x) = \left[\prod_{j=1}^{s} (x^{p_j^{a_j}} - x)^{2n}\right](x - 1)$$

where, of course $p_1, p_2, \cdots, p_s$ are the distinct prime factors of q. Observe that the coefficient of the lowest degree term in $u(x)$ is -1. Moreover, by (27), if x is any element of any of the rings R_i $(i \in \Gamma)$, $u(x) = 0$. Hence, in view of the fact that the operations of a subdirect sum are componentwise, $u(x) = 0$ for all x in the ground ring R. Thus, by (28) we see that, for some integer $m > 1$ and some monic polynomial $g(x)$ with integer coefficients equation (24) holds, and the lemma is proved.

LEMMA 6. *Suppose that R is a ring of positive characteristic q and with unity element. Then,*

$$(29) \qquad x^{\check{}} = x^{\hat{}\,q-1} \quad \textit{and} \quad x \times_{\hat{}} y = (x^{\hat{}} \times y^{\hat{}})^{\hat{}\,q-1} .$$

Moreover, any monic polynomial $f(x)$ with integer coefficients and zero constant term is expressible in terms of the operations $\times$ and $\hat{}$ in R.

Proof. To avoid any possible confusion, let us denote the unity of R by e. Then $x^{\hat{}} = x + e$ and $x^{\check{}} = x - e$. Hence, (see (4)),

$$x^{\hat{}\,q-1} = x + (q - 1)e = x - e = x^{\check{}} .$$

Now recalling the definition of $\times_{\hat{}}$ in (5) we have

$$x \times_{\hat{}} y = (x^{\hat{}} \times y^{\hat{}})^{\check{}} = (x^{\hat{}} \times y^{\hat{}})^{\hat{}\,q-1}$$

which proves (29).

To complete the proof of the lemma, consider the monic polynomial

$$(30) \qquad f(t) = t^n + a_1 t^{n-1} + a_2 t^{n-2} + \cdots + a_{n-1} t$$

with integer coefficients and zero constant term. Since by hypothesis

the characteristic of R is q, $qx = 0$ for all $x \in R$. Thus we may assume, without loss of generality, that *each of the integers* a_i $(i = 1, 2, \cdots, n-1)$ *in* (30) *is positive.* Then, by (4), we see that

$$f(x) = x(\cdots(x(x(x^{\wedge a_1})^{\wedge a_2})^{\wedge a_3})\cdots)^{\wedge a_{n-1}} .$$

This finishes the proof of the lemma.

With the aid of these lemmas we are now in a position to prove the following main theorem.

THEOREM 2. *Let R be a ring with unity* 1; *let n be a fixed positive integer, and let $f(t)$ be a fixed polynomial with integer coefficients such that for all $x \in R$*

$$x^n = x^{n+1}f(x) . \tag{31}$$

If, further, all the idempotent elements of R commute with each other, then the "$+$" of R is equationally definable in terms of the "$\times$" of R and the (unary) successor operation $\wedge$.

Proof. By Lemma 5 there exists a *monic* polynomial $g(t)$ with integer coefficients and an integer $m > 1$ such that $x^m = x^{m+1}g(x)$ for all $x \in R$. We claim that R satisfies the following identity:

$$\begin{cases} x + y = [x(x^{m-1}(g(x))^m y)^\wedge (xg(x))^m] \times_\wedge \\ \qquad [x^\wedge((x^\wedge)^{m-1}(g(x^\wedge))^m y^\vee)^\wedge(((xg(x))^m)^\vee)^2] . \end{cases} \tag{32}$$

To prove this we recall first that by Lemma 3, R is isomorphic to a subdirect sum of *local* rings R_i $(i \in \Gamma)$. Since the operations in a subdirect sum are componentwise it suffices to verify (32) for each local ring R_i. To this end we distinguish two cases:

Case 1. x is a unit in R_i. Note that $x^m = x^{m+1}g(x)$ holds in R_i and hence $xg(x) = 1$. Therefore the right side of (32) reduces to (see (3))

$$[x(1 + x^{m-1}(g(x))^m y)] \times_\wedge 0 ,$$

since $(((xg(x))^m)^\vee)^2 = (1^\vee)^2 = 0^2 = 0$. But then the right side (see (6)) reduces to

$$x + x^m(g(x))^m y = x + (xg(x))^m y = x + y$$

as desired.

Case 2. x is a nilpotent element in R_i—the only other possibility in a local ring. In this case $1 + x = x^\wedge$ is a unit in R_i. Therefore, as in Case 1, we have $x^\wedge g(x^\wedge) = 1$. Moreover, since $x^m = x^{m+1}g(x)$,

by reiterating we get

$$x^m = x^{m+r}(g(x))^r \tag{33}$$

for all positive integers r. Since x is nilpotent, (33) readily implies that $x^m = 0$, and, therefore, $(xg(x))^m = 0$. Thus, the right side of (32) reduces to

$$\begin{aligned} 0 \times_{\wedge} [x^{\wedge}(1 + (x^{\wedge})^{m-1}(g(x^{\wedge}))^m y^{\vee})(0^{\vee})^2] \\ = (x^{\wedge} + (x^{\wedge})^m(g(x^{\wedge}))^m y^{\vee})(-1)^2 \\ = x^{\wedge} + (x^{\wedge} g(x^{\wedge}))^m y^{\vee} = x^{\wedge} + y^{\vee} \\ = x + y \,. \end{aligned}$$

These two cases demonstrate that (32) is an identity satisfied by all elements x and y of each local ring R_i $(i \in \Gamma)$. Therefore, (32) is an identity of the ground ring R.

To complete the proof, we first observe that by setting $x = 2$ in (31), we get

$$2^n = 2^{n+1} f(2) \,.$$

Thus, the characteristic of R is a positive integer q. Hence, by (2)-(5),

$$x^{\vee} = x^{\wedge q-1} \quad \text{and} \quad x \times_{\wedge} y = (x^{\wedge} \times y^{\wedge})^{\wedge q-1} \,. \tag{34}$$

Now let

$$h(t) = t^{m-1}(g(t))^m \,. \tag{35}$$

Note that since $g(t)$ is a monic polynomial with integer coefficients and $m > 1$, $h(t)$ is also a monic polynomial with integer coefficients whose constant term is zero. Therefore, by Lemma 6, $h(t)$ is expressible as a primitive composition of the operations $\times$ and $^{\wedge}$, say

$$h(t) = \Phi(t; \times, ^{\wedge}) \,. \tag{36}$$

By (35) and (36), it follows that

$$x^{m-1}(g(x))^m = \Phi(x; \times, ^{\wedge}) \quad \text{and} \quad (x^{\wedge})^{m-1}(g(x^{\wedge}))^m = \Phi(x^{\wedge}; \times, ^{\wedge}) \,. \tag{37}$$

Also by Lemma 6, $xg(x)$ is expressible as a primitive composition of the operations $\times$ and $^{\wedge}$, say

$$xg(x) = \psi(x; \times, ^{\wedge}) \,. \tag{38}$$

In view of (34), (37), and (38), the right side of the identity (32) is expressible in terms of the two operations $\times$, and $^{\wedge}$, which proves the theorem.

3. Examples. We turn now to some examples of rings, some commutative and some not commutative, to which our theorems apply.

EXAMPLE 1. Let R be any Boolean ring with unity [5]; more generally, let R by any p-ring with unity; i.e., R satisfies $x^p = x$, $px = 0$, p = prime. (See [4], [2], and [7].) Then the "$+$" of R is equationally definable in terms of "$\times$" and "$\hat{}$".

EXAMPLE 2. Let R be any ring with unity in which, for a fixed $n > 1$ and every $x \in R$, $x^n = x$. Then here too the "$+$" of R is equationally definable in terms of "$\times$" and "$\hat{}$".

It should be pointed out that the rings of Examples 1 and 2 are necessarily *commutative*, (see [3]; p. 217), as are, of course the rings of the next example.

EXAMPLE 3. Let R be the ring Z_n of integers modulo n. It can be shown that R is periodic; in fact, R satisfies the identity

$$x^{n\varphi(n)} = x^{2n\varphi(n)}$$

where $\varphi(n)$ is the familiar Euler φ-function. Therefore, by Theorem 1, the "$+$" of R is equationally definable in terms of "$\times$" and $\hat{}$. Indeed equation (7) now becomes

$$x + y = [x(x^{n\varphi(n)-1}y)\hat{}(x^{(n\varphi(n))^2})] \times_{\hat{}} [x\hat{}((x\hat{})^{n\varphi(n)-1}y\check{})\hat{}((x^{(n\varphi(n))^2})\check{})^2] .$$

This formula for "$+$" is much simpler than that given in [6].

The next two examples demonstrate that our theorems also apply to some rings which are *not* commutative.

EXAMPLE 4. Let $F = GF(p^k)$ be a finite field and let R be the ring of those $n \times n$ upper triangular matrices over F in which all of the entries on the main diagonal are equal. It can be shown that R is a finite local ring whose only idempotent elements are the zero matrix and the identity matrix. The ring R is also a periodic ring; in fact, R satisfies the following identity:

$$x^{p^{nk}} = x^{p^{(n+1)k}} .$$

Therefore R satisfies all of the hypotheses of Theorem 1; and hence, the "$+$" of R is equationally definable in terms of "$\times$" and $\hat{}$. Observe that R is *not* commutative for $n > 2$ even over $GF(2)$.

Example 4 can be generalized as follows.

EXAMPLE 5. Let R be any *finite* (not necessarily commutative) ring in which all of the idempotent elements commute with each other. Then the "$+$" of R is equationally definable in terms of "$\times$" and $\hat{}$.

To prove this we let $R = \{x_1, x_2, \cdots, x_k\}$. Now for any $x_i \in R$ let

$$S = \{x_i, x_i^2, \cdots, x_i^{k+1}\} .$$

Since S contains $k + 1$ elements of R, there must exist integers r_i and s_i such that $1 \leqq r_i < s_i \leqq k + 1$ for which

$$x_i^{r_i} = x_i^{s_i} .$$

Therefore, as in the proof of Lemma 1(i), it must follow that $x_i^{(s_i - r_i)r_i}$ is idempotent. Now let

$$n = \prod_{i=1}^{k} (s_i - r_i)r_i \quad \text{and} \quad m = 2n .$$

Then we see that each $x \in R$, $x^m = x^n$. Hence, R is periodic. Therefore, again by Theorem 1, the "$+$" of R is equationally definable in terms of the "$\times$" of R and the successor operation $\hat{}$.

The rings in Examples 4 and 5 are the first known examples of rings in which the commutative operation of ring addition is equationally definable in terms of a *not* commutative ring multiplication and a successor operation $\hat{}$. One might ask just how noncommutative a ring may be for this to still be possible.

In conclusion, we would like to express our indebtedness and gratitude to the referee for his helpful suggestions and valuable comments.

REFERENCES

1. G. Birkhoff, *Subdirect unions in universal algebras*, Bull. Amer. Math. Soc., **50** (1944), 764-768.
2. A. L. Foster, *p-rings and ring-logics*, University of California Publ., **1** (1951), 385-396.
3. N. Jacobson, *Structure of rings*, Amer. Math. Colloq. Publ., **37** (1964).
4. N. H. McCoy and D. Montgomery, *A representation of generalized Boolean rings*, Duke Math. J., **3** (1937), 455-459.
5. M. H. Stone, *The theory of representations of Boolean algebras*, Trans. Amer. Math. Soc., **40** (1936), 37-111.
6. A. Yaqub, *On the theory of ring-logics*, Canad. J. Math., **8** (1956), 323-328.
7. ———, *On certain finite rings and ring-logics*, Pacific J. Math., **12** (1962), 785-790.

Received February 16, 1977 and in revised form August 15, 1977.

BRIGHAM YOUNG UNIVERSITY AT PROVO, UT 84112
AND
UNIVERSITY OF CALIFORNIA AT SANTA BARBARA, CA 93106