JOURNAL OF ALGEBRA 92, 1–8 (1985)

Equational Definability of Addition in Certain Noncommutative Rings

MOHAN S. PUTCHA

Department of Mathematics, North Carolina State University, Raleigh, North Carolina 27650

AND

ADIL YAQUB

Department of Mathematics, University of California, Santa Barbara, California 93106

Communicated by P. M. Cohn

Received May 8, 1981

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, any ring R with unity, *not necessarily commutative*, which 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. This class, of course, contains all finite rings with unity. As a corollary it is shown that if $S \subseteq R$ and $1 \in S$, and if along with $a, b \in S$, $ab \in S$ and $a + 1 \in S$, then S is a subring of R. © 1985 Academic Press, Inc.

I. INTRODUCTION

The main purpose of this paper is to establish the *equational* definability of addition in terms of multiplication and the successor operation for a rather wide class of noncommutative rings, a class which subsumes Boolean rings [3] as well as finite rings. In a series of papers [4–6] one of the authors proved that such equational definability holds in certain classes of commutative rings, while in [1] and [2] it was shown that some rings which are not commutative but have their idempotents in the center also enjoy this property. Our present objective is to prove the following theorem which contains and substantially generalizes all of these results. Indeed, we prove the following:

0021-8693/85 $3.00

THEOREM 1. *Let R be a ring with unity* 1, *not necessarily commutative. Let n be a fixed positive integer, and let $f(t)$ be a fixed polynomial with integer coefficients such that*

$$x^n = x^{n+1}f(x) \qquad \text{for all } x \text{ in } R. \tag{1.1}$$

Then the "+" of R is equationally definable in terms of the "$\times$" of R and the (unary) successor operation "$\wedge$".

In preparation for the proof of Theorem 1, we first introduce some notation and prove some lemmas. As stated above, for any x in R, we define

$$x^{\wedge} = x + 1 \tag{1.2}$$

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

$$x^{\vee} = x - 1. \tag{1.3}$$

We also use the notation

$$x^{\wedge k} = (\ldots((x^{\wedge})^{\wedge})^{\wedge}\ldots)^{\wedge} \qquad (k \text{ iterations}). \tag{1.4}$$

The proof of Theorem 1 utilizes the *commutative* version of Theorem 1 which was proved in [2]. We state this formally as

LEMMA 1. *Let R be a ring with unity* 1, *not necessarily commutative, and suppose R satisfies all the hypotheses of Theorem* 1. *Suppose R_0 is any commutative subring of R and suppose $1 \in R_0$. Then the "+" of R_0 is equationally definable in terms of the "$\times$" of R_0 and the successor operation "$\wedge$".*

LEMMA 2. *Under all the hypotheses of Theorem* 1, *there exists a positive integer m such that*

$$ma = 0 \qquad \text{for all } a \text{ in } R, \tag{1.5}$$

and hence

$$a^{\vee} = a^{\wedge m-1} \qquad \text{for all } a \text{ in } R. \tag{1.6}$$

Proof. By (1.1), $2^n = 2^{n+1}f(2)$. Now, let $m = |2^{n+1}f(2) - 2^n|$ and recall that, by (1.3),

$$a^{\vee} = a - 1 = a + (m-1) = a^{\wedge m-1} \qquad \text{(see (1.4) and (1.2)).}$$

LEMMA 3. *Under all the hypotheses of Theorem* 1 *and with any fixed*

positive integer k, there exists a primitive composition $\Pi(x)$, composed of the operations "$\times$" and "$\wedge$" such that

$$\Pi(a) = ka \qquad \textit{for all } a \textit{ in } R. \tag{1.7}$$

Proof. Let $a \in R$, and let

$$R_0 = \langle a, 1 \rangle = \text{subring of } R \text{ generated by } a \text{ and } 1.$$

By Lemma 1, there exists a primitive composition $\Phi(x, y)$, composed of the operations "$\times$" and "$\wedge$", such that

$$x_0 + y_0 = \Phi(x_0, y_0) \qquad \text{for } \textit{all } x_0, y_0 \text{ in } R_0. \tag{1.8}$$

In particular

$$2a = a + a = \Phi(a, a),$$
$$3a = 2a + a = \Phi(2a, a) = \Phi(\Phi(a, a), a), \qquad \text{etc.}$$

Continuing this process, we eventually obtain (1.7), and the lemma is proved.

An extremely useful special case of Lemma 3 is

COROLLARY 1. *Suppose that the ring R satisfies all the hypotheses of Theorem* 1. *Then there exists a primitive composition $\Pi(x)$ composed of the operations "$\times$" and "$\wedge$" such that*

$$\Pi(a) = -a \qquad \textit{for all } a \textit{ in } R.$$

Proof. By (1.5), $-a = (m-1)a$. Now apply Lemma 3. (Note that in Lemma 2, $m = |2^{n+1}f(2) - 2^n| \geqslant 2$.)

LEMMA 4. *Under all the hypotheses of Theorem* 1 *and for any fixed polynomial $g(x)$ with integer coefficients, there exists a primitive composition $\psi(x)$, composed of the operations "$\times$" and "$\wedge$", such that*

$$g(a) = \psi(a) \qquad \textit{for all } a \textit{ in } R. \tag{1.9}$$

Proof. In view of Lemma 2, assume without loss of generality that all the coefficients of $g(x)$ are *positive*. Let

$$g(x) = c_0x^k + c_1x^{k-1} + c_2x^{k-2} + \cdots + c_{k-1}x + c_k,$$

all c_i are positive integers.

Recalling (1.4), we readily verify that

$$g(x) = (x(...(x(x(x(c_0x)\wedge c_1)\wedge c_2)\wedge c_3)\wedge c_4 ...)\wedge c_{k-1})\wedge c_k.$$

Moreover, by Lemma 3, there exists a promitive composition $\Pi(x)$, composed of "$\times$" and "$\wedge$", such that

$$\Pi(a) = c_0 a \qquad \text{for } \textit{all } a \textit{ in } R.$$

Thus, if we define

$$\psi(x) = (x(...(x(x(x(\Pi(x))\wedge c_1)\wedge c_2)\wedge c_3)\wedge c_4 ...)\wedge c_{k-1})\wedge c_k,$$

we see that (1.9) holds, and the lemma is proved.

Although the following lemma is a special case of Lemma 4, we single it out in view of its important role in the remaining proofs.

LEMMA 5. *For any positive integer i, there exists a primitive composition $\xi_i(x)$, composed of* "$\times$" *and* "$\wedge$", *such that*

$$1 + a + a^2 + \cdots + a^i = \xi_i(a) \qquad \textit{for all } a \textit{ in } R. \tag{1.10}$$

To illustrate (1.10), note that $1 + a + a^2 = (aa^{\wedge})^{\wedge}$, $1 + a + a^2 + a^3 = (a(aa^{\wedge})^{\wedge})^{\wedge}$, etc. Continuing this process, we eventually obtain (1.10) for any given i.

LEMMA 6. *For any a, b in R with $a^{i+1} = 0$, we have*

$$a + b = [a^{\vee}\{(\xi_i(a))(-b)\}^{\wedge}]^{\wedge} = [a^{\wedge_{m-1}}\{(\xi_i(a))\,\Pi(b)\}^{\wedge}]^{\wedge}, \tag{1.11}$$

where $\xi_i(a)$ ia as in (1.10), *$\Pi(b)$ is as in Corollary* 1, *and m is as in Lemma* 2. *Thus, $a + b$ is a primitive composition of a and b via the operations* "$\times$" *and* "$\wedge$"..

Proof. Follows at once by expanding the right side of (1.11).

LEMMA 7. *Suppose R satisfies all the hypotheses of Theorem* 1. *Then there exists a primitive composition $\lambda(x, y)$ composed of* "$\times$" *and* "$\wedge$", *such that*

$$a - e = \lambda(e, a) \qquad \textit{for all } a, e \textit{ in } R \textit{ with } e^2 = e. \tag{1.12}$$

Proof. First, observe that (see (1.3) and (1.6))

$$-e + eae = e(ae)^{\vee} = e(ae)^{\wedge_{m-1}}, \tag{1.13}$$

$$a - ea = (-e)^{\wedge}a = (\Pi(e))^{\wedge}a \qquad \text{(see Corollary 1).} \tag{1.14}$$

Moreover, as is readily verified,

$$a - e + eae - ea = [(-e + eae)^{\wedge}(a - ea)^{\wedge}]^{\vee}. \tag{1.15}$$

Combining (1.15), (1.13), (1.14), and (1.6), we get

$$a - e + eae - ea = [(e(ae)^{\wedge_{m-1}})^{\wedge}((\Pi(e))^{\wedge}a)^{\wedge}]^{\wedge_{m-1}}. \tag{1.16}$$

Also, by Corollary 1,

$$ea - eae = ea(-e)^{\wedge} = ea(\Pi(e))^{\wedge} \qquad \text{and} \qquad (ea - eae)^2 = 0. \tag{1.17}$$

Now, observe that

$$a - e = (a - e + eae - ea) + (ea - eae). \tag{1.18}$$

Let

$$b = a - e + eae - ea, \qquad a_0 = ea - eae. \tag{1.19}$$

Then (1.18) yields

$$a - e = a_0 + b, \qquad \text{where} \quad a_0^2 = 0. \tag{1.20}$$

By (1.20), Lemma 6, and (1.10) with $i = 1$, we see that (1.11) reduces to

$$a_0 + b = [a_0^{\wedge_{m-1}}\{a_0^{\wedge}\Pi(b)\}^{\wedge}]^{\wedge}. \tag{1.21}$$

Combining (1.16)–(1.21), we see that (1.12) holds and the lemma is proved.
We are now in a position to prove Theorem 1.

Proof of Theorem 1. Let a and b be arbitrary elements of R, and let

$$R_0 = \langle a, 1\rangle = \text{subring of } R \text{ generated by } a \text{ and } 1. \tag{1.22}$$

By hypothesis, $a^n = a^{n+1}f(a)$ and hence $a^n = a^{2n}(f(a))^n$. Let

$$e = a^n = a^n(f(a))^n, \quad c = ea = ae, \quad w = a^n(f(a))^{n+1}, \quad d = a - c. \tag{1.23}$$

Then, as in readily verified,

$$ew = we = w, \qquad cw = wc = e, \qquad ec = ce = c, \qquad e^2 = e. \tag{1.24}$$

Moreover, by (1.23) and Lemma 4,

$$\begin{gathered} e, c, w, d \text{ are all primitive compositions of } a \\ \text{via the operations "}\times\text{" and "}\wedge\text{".} \end{gathered} \tag{1.25}$$

Now, $a^n e = a^{2n}(f(a))^n = a^n$ (see above), and thus $a^n(1-e) = 0$. Since $c = ae = ea$, we have

$$d^n = (a-c)^n = (a-ae)^n = a^n(1-e)^n = 0. \tag{1.26}$$

Moreover, by (1.25) and (1.22),

$$e, c, w, d \text{ are all in the } \textit{commutative} \text{ subring } R_0. \tag{1.27}$$

Hence, by Lemma 1, there exists a primitive composition $\delta(x, y)$, composed of "$\times$" and "$\wedge$", such that

$$a_0 + b_0 = \delta(a_0, b_0) \qquad \text{for } \textit{all } a_0 \text{ and } b_0 \text{ in } R_0. \tag{1.28}$$

By (1.27) and (1.28), we see that (see (1.6))

$$w + e - 1 = (\delta(w, e))^{\vee} = (\delta(w, e))^{\wedge_{m-1}}, \tag{1.29}$$

$$c + e - 1 = (\delta(c, e))^{\vee} = (\delta(c, e))^{\wedge_{m-1}}. \tag{1.30}$$

Moreover, it can be checked that (see (1.24))

$$[(c+e-1)\{(w+e-1)b\}^{\wedge}]^{\wedge} = c + e + b. \tag{1.31}$$

Combining (1.31), (1.30), (1.29), and (1.25), we conclude that

$$\begin{gathered} c + e + b \text{ is a primitive composition of } a \text{ and } b \\ \text{via the operations "}\times\text{" and "}\wedge\text{".} \end{gathered} \tag{1.32}$$

Now, combining (1.32) and Lemma 7 (recall that $e^2 = e$), we have

$$\begin{gathered} c + b = (c + e + b) - e = \lambda(e, c + e + b), \text{ where } \lambda(x, y) \\ \text{is a primitive composition of } x \text{ and } y \text{ via "}\times\text{" and "}\wedge\text{".} \end{gathered} \tag{1.33}$$

In view of (1.33), (1.32), and (1.25), we see that

$$c + b \text{ is a primitive composition of } a \text{ and } b \text{ via "}\times\text{" and "}\wedge\text{".} \tag{1.34}$$

Finally, since $d = a - c$ (see (1.23)), we have $a + b = (c + b) + d$, and $d^n = 0$ (see (1.26)). Hence, by Lemma 6 (note that $i + 1 = n$ is *fixed*), we conclude that

$$\begin{gathered} a + b \text{ is a primitive composition of } c + b \text{ and } d \\ \text{via the operations "}\times\text{" and "}\wedge\text{".} \end{gathered} \tag{1.35}$$

Combining (1.35), (1.34), and (1.25), we see that

$$\begin{aligned} &a + b = \theta(a, b) \text{ for some primitive composition} \\ &\theta(x, y), \text{ composed of the operations "}\times\text{" and "}\wedge\text{".} \end{aligned} \tag{1.36}$$

Finally, we must show that θ can be chosen to be independent of a and b. To see this, let R_1 denote the free ring with unity in two noncommuting indeterminates X, Y subject to the identity $u^n \equiv u^{n+1} f(u)$. Then, by (1.36), there exists a primitive composition $\theta(x, y)$ composed of the operations "$\times$" and "$\wedge$" such that $X + Y = \theta(X, Y)$. Let $a, b \in R$ be arbitrary. Then the map $X \to a$, $Y \to b$ extends to a homomorphism from R_1 into R. Therefore, $a + b = \theta(a, b)$. This proves the theorem.

We conclude this paper with the following corollaries, which are of independent interest.

COROLLARY 2. *Let S be a subset of a ring R, where R satisfies the hypotheses of Theorem* 1. *Suppose that $1 \in S$ and for all $a \in S$, $b \in S$, we have $ab \in S$ and $a + 1 \in S$. Then S is a subring of R.*

COROLLARY 3. *Suppose R is a finite ring with unity* 1, *and $S(\times)$ is a subgroup of R with the property that $a \in S$ implies $a + 1 \in S$. Then $S(\times, +)$ is a subring of R.*

Proof. Since R is finite, there exists a positive integer m such that

$$mr = 0 \qquad \text{for all} \quad r \in R. \tag{1.37}$$

The finiteness of R can also be seen to imply that R satisfies the identity $u^n = u^{n+1} f(u)$ for some $n \in \mathbb{Z}^+$ and some $f(x) \in \mathbb{Z}[x]$. In view of Corollary 2, it suffices to show that

$$1 \in S. \tag{1.38}$$

To prove (1.38), first observe that by (1.37) and one of our hypotheses,

$$s - 1 = s + (m - 1)\, 1 \in S \qquad \text{for all} \quad s \in S. \tag{1.39}$$

Let $a \in S$ and let $a^p = a^q$, $p > q \geqslant 1$. Then, using (1.39) and the hypothesis that $S(\times)$ is a semigroup,

$$0 = a^q(a^{p-q} - 1) \in S.$$

Thus, $0 \in S$ and hence by hypothesis, $1 = 0 + 1 \in S$, which proves (1.38). This completes the proof.

REFERENCES

1. H. ABY-KHUZAM, H. TOMINAGA, AND A. YAQUB, Equational definability of addition in rings satisfying polynomial identities, *Math. J. Okayama Univ.* **22** (1980), 55–57.
2. H. G. MOORE AND A. YAQUB, Equational definability of addition in certain rings, *Pacific J. Math.* **74** (1978), 407–417.
3. M. H. STONE, The theory of representations of Boolean algebras, *Trans. Amer. Math. Soc.* **40** (1936), 37–111.
4. A. YAQUB, On the theory of ring-logics, *Canad. J. Math.* **8** (1956), 323–328.
5. A. YAQUB, On certain finite rings and ring-logics, *Pacific J. Math.* **12** (1962), 785–790.
6. A. YAQUB, Ring-logics and residue class rings, *Pacific J. Math.* **15** (1965), 1465–1469.