

Mathematical Journal of Okayama University

Volume 24, Issue 2

1982

Article 4

DECEMBER 1982

On the equational definability of addition in rings

Hiroaki Komatsu*

*Osaka City University

Copyright ©1982 by the authors. *Mathematical Journal of Okayama University* is produced by
The Berkeley Electronic Press (bepress). <http://escholarship.lib.okayama-u.ac.jp/mjou>

ON THE EQUATIONAL DEFINABILITY OF ADDITION IN RINGS

HIROAKI KOMATSU

Boolean rings and Boolean algebras, though conceptually different, were shown by Stone [6] to be equationally interdefinable. Indeed, in a Boolean ring, addition can be defined in terms of the ring multiplication and the Boolean complementation “*”. Recently, Putcha and Yaquub [5] have shown that the equational definability of addition in terms of the ring multiplication and the successor operation “^” also holds for rings satisfying a polynomial identity $X^m - X^{m+1}f(X) = 0$, where $m \geq 1$ and $f(X) \in \mathbf{Z}[X]$. The purpose of this paper is to give a shorter proof of the above result and show that the converse is also true. Furthermore, we shall reprove the main theorem of our previous paper [4].

Throughout the present paper, R will represent a ring with identity element 1. For any $a \in R$, we define $a^\wedge = a + 1$, $a^\vee = a - 1$ and $a^* = 1 - a$. We also use the notation $\sigma_k(a) = (\cdots a(aa^\wedge)^\wedge \cdots)^\wedge = a^k + a^{k-1} + \cdots + 1$. Let $\mathbf{Z}\{X\}$ be the free ring generated by $X = \{X_1, \cdots, X_r\}$, and T a set of unary operations in $\mathbf{Z}\{X\}$. We set

$$C_0(X; T) = X, \text{ and}$$

$$C_{n+1}(X; T) = \{(\psi_1 \cdots \psi_s)^{\tau_1 \cdots \tau_t} \in \mathbf{Z}\{X\} \mid \psi_i \in C_n(X; T), \tau_j \in T, s \geq 1, t \geq 0\}.$$

Obviously, $C_0(X; T) \subseteq C_1(X; T) \subseteq \cdots$, and $C(X; T) = \bigcup_{n=0}^{\infty} C_n(X; T)$ is the set of all primitive compositions composed of the ring multiplication of $\mathbf{Z}\{X\}$ and T . Now, let f be in $\mathbf{Z}\{X\}$. If f has only one monomial p of the highest degree and the coefficients of p is 1, we call f a monic polynomial, and p the leading term of f .

We start with the following lemma.

Lemma 1. (1) If $\psi = \psi(X_1, \cdots, X_r)$ is in $C(X; ^\wedge, ^\vee)$ then ψ is a monic polynomial and every X_k , occuring in ψ , also occurs in the leading term of ψ .

(2) If $\psi = \psi(X_1, \cdots, X_r)$ is in $C(X; *)$ then $\psi(1, \cdots, 1) = 0$ or 1, where 1 is the identity element in R .

Proof. (1) Suppose that ψ is in $C_{n+1}(X; ^\wedge, ^\vee)$. Then we can write $\psi = \psi_1 \cdots \psi_s + \alpha$ with $\psi_i \in C_n(X; ^\wedge, ^\vee)$ and $\alpha \in \mathbf{Z}$. Hence, the assertion is easily seen by induction.

(2) Suppose that ϕ is in $C_{n+1}(X;*)$. Since $\phi = \phi_1 \cdots \phi_s$ or $1 - \phi_1 \cdots \phi_s$ with some $\phi_i \in C_n(X;*)$, the assertion is easily seen by induction.

Lemma 2. *Let a, b be elements of R . If b is nilpotent; $b^n = 0$ say, then $a - b = -\{(a\sigma_{n-1}(b))^\wedge b^\vee\}^\wedge$.*

Proof. Since $\sigma_{n-1}(b) = (1 - b)^{-1} = -(b^\vee)^{-1}$, the assertion is easily seen.

Lemma 3. *Let a be a strongly π -regular element of R ; $a^n = a^{2n}s = ta^{2n}$ with a positive integer n and $s, t \in R$. Then there exists a primitive composition $\theta(X, Y, Z)$, composed of the " $\cdot$ ", " $\wedge$ " and " $\vee$ ", such that $a + b = \theta(a, b, s)$ for all $b \in R$.*

Proof. By the proof of [2, Lemma 1], we see that $e = a^n s$ is an idempotent such that $ae = ea$ and $a^n e = a^n$. Set $c_1 = e^\vee b e^\vee$, $c_2 = ea + eb = ea(a^{n-1}sb)^\wedge$, $c_3 = e^\vee a$, and $c_4 = e^\vee be$. Since $a + b = c_1 + c_2 - c_3 - c_4$ and $c_1 c_2 = c_3^2 = c_4^2 = 0$, by Lemma 2 we find that

$$a + b = [(((c_1^\wedge c_2^\wedge)^\vee \sigma_{n-1}(c_3))^\wedge c_3^\vee)^\wedge c_4^\wedge]^\vee c_4^\vee,$$

which completes the proof.

Here, as application of Lemma 3, we reprove Theorem and Corollary 1 of [4].

Corollary 1. *Let S be a multiplicative subsemigroup of R . Suppose that, for any $a \in S$, a is right π -regular in S and left π -regular in R and $-a, a+1 \in S$. Then S is a subring of R .*

Proof. By hypothesis, $x \in S$ always implies $x^\wedge, x^\vee \in S$. Thus, if $\phi(X, Y, Z)$ is in $C(X, Y, Z;^\wedge,^\vee)$ then $\phi(x, y, z) \in S$ for all $x, y, z \in S$. Now, let a be an arbitrary element of S . Since a is strongly π -regular and is right π -regular in S , by Lemma 3 there exist $s \in S$ and $\theta(X, Y, Z) \in C(X, Y, Z;^\wedge,^\vee)$ such that $a + b = \theta(a, b, s)$ for all $b \in S$.

Corollary 2. *Let R be a right integral extension of a division ring D . Let S be a multiplicative subsemigroup of R . Suppose that S contains D and suppose, further, that $a \in S$ always implies that $a+1 \in S$. Then S is a subring of R .*

Proof. Let a be an arbitrary element of R . Since R is a right integral extension of D , we can easily see that $a^m = a^{m+1}a_0$ with some positive integer m and some $a_0 \in \sum_{i=0}^\infty a^i D$. Hence, by [3, Proposition 2], R is

strongly π -regular. Henceforth, we let a be an arbitrary element of S . Since every element of $\sum_{i=0}^{\infty} a^i D$ is of the form $a^k(a^h \alpha_h + \cdots + 1)\alpha$ ($\alpha, \alpha_j \in D$), an easy induction proves that $\sum_{i=0}^{\infty} a^i D \subseteq S$. Thus, $a^n = a^{2n}b = ca^{2n}$ for some positive integer n and some $b \in S$ and $c \in R$. Thus, by Corollary 1, S is a subring of R .

We now prove the main theorem, which is stated as follows:

Theorem 1. *The following statements are equivalent:*

- 1) *R satisfies a polynomial identity $X^{2n} - X^n = 0$ with some positive integer n .*
- 2) *R satisfies a polynomial identity $f(X) = 0$ with a primitive polynomial $f(X)$ in $\mathbb{Z}[X]$.*
- 3) *The "+" of R is equationally definable in terms of the "." of R and " $\wedge$ ".*
- 4) *The "+" of R is equationally definable in terms of the "." of R and " $\vee$ ".*
- 5) *The "+" of R is equationally definable in terms of the "." of R , " $\wedge$ " and " $\vee$ ".*

Proof. Obviously, $1) \Rightarrow 2)$, $3) \Rightarrow 5)$, and $4) \Rightarrow 5)$.

$2) \Rightarrow 1)$. Since the equation $f(X) = 0$ has only a finite number of solutions in $\mathbb{Z}$, R has finite characteristic q . Let $q = p_1^{e_1} \cdots p_r^{e_r}$, where p_i are distinct primes and the $e_i > 0$. Then, it is easy to see that the ring $p_1^{e_1} \cdots p_{i-1}^{e_{i-1}} R / p_1^{e_1} \cdots p_i^{e_i} R$ satisfies a polynomial identity $f_i(X) = 0$ with a monic $f_i(X) \in \mathbb{Z}[X]$. Thus, without loss of generality, we may assume that $f(X)$ is monic. Then, setting $n = \deg f(X)$, we have $| \langle a \rangle | < q^n$ for all $a \in R$. Hence, there holds 1), by [1, Lemma].

$1) \Rightarrow 3)$ and $4)$. By Lemma 3, there exists $\theta(X, Y, Z)$ in $C(X, Y, \mathbb{Z}; \wedge, \vee)$ such that $a + b = \theta(a, b, a^n)$ for all $a, b \in R$. Since $q = |2^{2n} - 2^n| \geq 2$ in $\mathbb{Z}$ and $qR = 0$, we have $x^\vee = x + (q-1) = (\cdots (x^\wedge)^\wedge \cdots)^\wedge$ and $x^\wedge = (\cdots (\cdots (x^\vee)^\vee \cdots)^\vee)^\vee$, $q-1$ iterations. This proves 3) and 4).

$5) \Rightarrow 2)$. There exists $\theta(X, Y) \in C(X, Y; \wedge, \vee)$ such that $a + b = \theta(a, b)$ for all $a, b \in R$. We can write $\theta(X, Y) = f(X, Y) + g(X) + h(Y) + \alpha$, where α is the constant term of $\theta(X, Y)$, $g(X) \in \mathbb{Z}[X]$ and $h(Y) \in \mathbb{Z}[Y]$ have no constant terms, and $f(X, Y)$ has no monomials of one variable. Obviously, $0 = \theta(0, 0) = f(0, 0) + g(0) + h(0) + \alpha \cdot 1 = \alpha \cdot 1 (\in R)$. Accordingly, for any $a \in R$, $a = a + 0 = \theta(a, 0) = f(a, 0) + g(a) + h(0) = g(a)$, and similarly $a = h(a)$. Therefore, $a + b = \theta(a, b) = f(a, b) + g(a) + h(b) = f(a, b) + a + b$, whence it follows that $f(a, b) = 0$ for all $a, b \in R$. Since $g(X) \neq 0$ and $h(Y) \neq 0$,

$f(X, Y)$ is a monic polynomial of positive degree, by Lemma 1 (1). Hence, $f(X, X)$ is also a monic polynomial of positive degree, and R satisfies the polynomial identity $f(X, X)=0$.

Corollary 3. *The following statements are equivalent:*

1) R is of characteristic 2 and satisfies a polynomial identity $X^{2n}-X^n=0$ with some positive integer n .

2) The "+" of R is equationally definable in terms of the "." of R and "*".

Especially, if R is a reduced ring then 2) is equivalent to

1)' R can be embedded in some direct product of $\text{GF}(2^m)$'s.

Proof. In view of Theorem 1, it suffices to show that 2) implies that R is of characteristic 2. Suppose that there exists $\theta(X, Y) \in C(X, Y; *)$ such that $a+b=\theta(a, b)$ for all $a, b \in R$. Then, by Lemma 1 (2), we have $2=\theta(1, 1)=0$. The latter is obvious by Jacobson's commutativity theorem, since a reduced ring satisfies the polynomial identity $X^{2n}-X^n=0$ if and only if it does $X^{n+1}-X=0$.

Acknowledgement. The author is grateful to Professor H. Tominaga for his helpful suggestion.

REFERENCES

- [1] H. ABU-KHUZAM, H. TOMINAGA and A. YAQUB: Equational definability of addition in rings satisfying polynomial identities, *Math. J. Okayama Univ.* **22** (1980), 55—57.
- [2] G. AZUMAYA: Strongly π -regular rings, *J. Fac. Sci. Hokkaido Univ., Ser. I*, **13** (1954), 34—39.
- [3] Y. HIRANO: Some studies on strongly π -regular rings, *Math. J. Okayama Univ.* **20** (1978), 141—149.
- [4] H. KOMATSU: On a theorem of M.S. Putcha and A. Yaqub, *Math. J. Okayama Univ.* **24** (1982), 21—23.
- [5] M.S. PUTCHA and A. YAQUB: Equational definability of addition in certain noncommutative rings, *J. Algebra* (to appear).
- [6] M.H. STONE: The theory of representations of Boolean algebras, *Trans. Amer. Math. Soc.* **40** (1936), 37—111.

DEPARTMENT OF MATHEMATICS, OSAKA CITY UNIVERSITY
SUGIMOTO, SUMIYOSHI-KU, OSAKA 558, JAPAN

(Received January 18, 1982)