Math. J. Okayama Univ. 23 (1981), 203—204

EQUATIONAL DEFINABILITY OF ADDITION IN RINGS GENERATED BY IDEMPOTENTS

ADIL YAQUB

Boolean rings and Boolean algebras, though historically and conceptually different, were shown by Stone to be equationally interdefinable [3]. Indeed, in a Boolean ring, addition can be defined in terms of ring multiplication and the successor operation (Boolean complementation). We show that this type of equational definability of addition also holds in a much wider class of rings, namely commutative rings with identity which are generated by tneir idempotents. The proof utilizes the structure theory of rings and the following elementary number-theoretic results.

Lemma 1. *Let m, n be positive integers, and p a prime. If m divides n then $\phi(m)$ divides $\phi(n)$, where ϕ denotes the Euler ϕ-function. Furthermore, if $p^k \leq m$ for some positive integer k then $\phi(m!) \geq k$.*

In preparation for the proof of the main theorem, we first introduce some notations. Throughout, $(R, +, \times)$ will be a commutative ring with identity 1. Let $x, y \in R$, and define:

$x^\wedge = x+1$, $x^\vee = x-1$,

$x^{\wedge k} = (\cdots((x^\wedge)^\wedge)^\wedge\cdots)^\wedge$ (k-iterations).

$x \times_\wedge y = (x^\wedge \times y^\wedge)^\vee (= x+y+xy)$.

We are now in a position to prove the following:

Theorem. *Let R be a commutative ring with identity 1, and suppose that the ring R is generated by its idempotents. Then the "+" of R is equationally definable in terms of the "$\times$" of R and the successor operation "$\wedge$". Indeed, there exists a positive integer n such that for all x, $y \in R$*

$$(1) \qquad x+y=[x(x^{\phi(n)-1}y)^\wedge x^{\phi(n)}]\times_\wedge[x^\wedge((x^\wedge)^{\phi(n)-1}y^\vee)^\wedge((x^{\phi(n)})^\vee)^2],$$

where ϕ is the Euler ϕ-function. Furthermore, $x^\vee = x^{\wedge n-1}$ and thus $x \times_\wedge y = (x^\wedge \times y^\wedge)^{\wedge n-1}$.

Proof. By hypothesis, there exist certain idempotents $e_1, \cdots, e_{m-1}$ $(m>1)$ such that $-1 = e_1+\cdots+e_{m-1}$. Let $n = m!$.

It is well known that the ground ring R is isomorphic to a subdirect sum of subdirectly irreducible rings R_i $(i \in \Gamma)$, and, of course, each such

R_i inherits all the hypotheses of R. Moreover, since the operations in a subdirect sum are componentwise, it suffices to verify (1) for each R_i.

Since R_i is a commutative subdirectly irreducible ring, in R_i the image of each e_j is either 0 or 1, and hence there exists a positive integer $m' \leq m-1$ such that $-1 = m'\cdot 1$ in R_i. Therefore, R_i is of characteristic p^k (p a prime, $k \geq 1$) and $R_i \simeq \boldsymbol{Z}_{p^k}$ (= ring of integers modulo p^k). Obviously, $p^k \leq m'+1 \leq m$. Since p^k divides n, $\phi(p^k)$ divides $\phi(n)$ and $\phi(n) \geq k$ by Lemma 1. If x is a unit in R_i then $x^{\phi(p^k)} = 1$ by Fermat-Euler Theorem. On the other hand, if x is a non-unit in R_i then $x^k = 0$ and $(x^\wedge)^{\phi(p^k)} = 1$. Hence,

(2) $x^{\phi(n)} = 1$ if x is a unit in R_i,

(3) $x^{\phi(n)} = 0$ and $(x^\wedge)^{\phi(n)} = 1$ if x is a non-unit in R_i.

Now, substituting (2) and (3) into the right side of (1), it becomes

$$\begin{cases} x(x^{-1}y)^\wedge \times_\wedge 0 = x(1+x^{-1}y) = x+y & \text{if } x \text{ is a unit in } R_i \\ 0 \times_\wedge x^\wedge(1+(x^\wedge)^{-1}y^\vee) = x^\wedge + y^\vee = x+y & \text{if } x \text{ is a non-unit in } R_i. \end{cases}$$

Also, the latter assertion is obvious from the fact that p^k divides n. This proves the theorem.

Remark. Since the ring $\boldsymbol{Z}_q$ of integers modulo q satisfies all the hypotheses of our theorem, and since $-1 = (q-1)\cdot 1$, we have $n = q!$, and hence (1) now becomes

$$x+y = [x(x^{\phi(q!)-1}y)^\wedge x^{\phi(q!)}] \times_\wedge [x^\wedge((x^\wedge)^{\phi(q!)-1}y^\vee)^\wedge((x^{\phi(q!)})^\vee)^2].$$

This formula for "+" in $\boldsymbol{Z}_q$ is much simpler than that given in [4]. Related work can be found in [1] and [2].

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] 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.

UNIVERSITY OF CALIFORNIA
SANTA BARBARA, U.S.A.

(Received July 7, 1981)