COLLOQUIUM MATHEMATICUM

VOL. XXV 1972 FASC. 1

ALGEBRAIC FUNCTIONS ON p-RINGS

BY

A. ISKANDER (NASHVILLE, TENNESSEE)

1. Let A be a ring. A function $f\colon A^n \to A$ is said to enjoy the substitution property [1] on A, if whenever Θ is a congruence relation on A, $a_i, b_i \in A$ and $a_i \Theta b_i$, $1 \leqslant i \leqslant n$; $f(a_1, \ldots, a_n)\Theta f(b_1, \ldots, b_n)$. A function $g\colon A^n \to A$ is said to be *algebraic* [1] on A, if there are: a polynomial $h(x_1, \ldots, x_{n+m})(m \geqslant 0)$, built up from $x_1, \ldots, x_{n+m}$ by addition, subtraction and multiplication; m elements $c_1, \ldots, c_m$ of A, such that $g(a_1, \ldots, a_n) = h(a_1, \ldots, a_n, c_1, \ldots, c_m)$.

It is well known [1] that every algebraic function enjoys the substitution property. The converse is not always true; $f(x) = (x^2+x^4)/2$ has the substitution property on Z, the ring of all integers, but it is not algebraic on Z. In [2] G. Grätzer had shown that every function with the substitution property on a Boolean algebra is Boolean; in [3] he discussed the case of distributive lattices with 0 and 1. The aim of the present paper is to give a description to all functions with the substitution property on p-rings ($x^p = x, px = 0, p$ is fixed prime). It is again not true here that every function with the substitution property is algebraic. We conclude the present paper by giving an example of a function with the substitution property on a p-ring, which is not algebraic on the given ring.

Let A be a p-ring not necessarily with 1. Then A is a subdirect power [4] of Z_p, the prime field of characteristic p. Let I be the power of Z_p which appears in the subdirect representation of A. Denote by A_1 the subring of Z_p^I generated by A and 1, and let

$$A^* = \{x\colon x \in Z_I^p, xA \subseteq A\}.$$

It is clear that $A_1 \subseteq A^*$. We have

THEOREM. *If A is a p-ring, then a function has the substitution property on A iff it is the restriction to A of an algebraic function on A^*.*

COROLLARY 1. *Let A be a p-ring. Every function with the substitution property on A is algebraic on A iff $A_1 = A^*$.*

COROLLARY 2. *If A is a p-ring with 1, then every function with the substitution property on A is algebraic on A.*

COROLLARY 3 [2]. *Every function with the substitution property on a Boolean algebra is Boolean.*

Corollary 3 follows from Corollary 2 since a Boolean algebra is a 2-ring with 1. Corollary 2 follows from Corollary 1, since $1 \in A$ implies $A_1 A = A^*$. The proof of the Theorem and Corollary 1 will be given in the next section.

I would like to express my thanks to F. M. Yaqub for several valuable discussions.

2. If A is a p-ring, $a \in A$, then we write $ax^0 = a$. If $b \in A^n$, b_k is the k-th component of b, and if $i \in Z_p^n$, then

$$b^i = b_1^{i_1}, \ldots, b_n^{i_n}, \quad 0 = (0, \ldots, 0).$$

Every algebraic function on A is of the form

$$f(x) = \sum \{a_i x^i : i \in Z_p^n\},$$

where

$$a_i \in A_1, \quad i \neq 0, \quad i \in Z_p^n, \quad a_0 \in A.$$

LEMMA 1. *Let A be a p-ring and let B be a subring of A. If $a_i \in A$, $i \in Z_p$ and $\sum \{a_i x^i : i \in Z_p\} \in B$ for all $x \in Z_p$, then $a_i \in B$ for all $i \in Z_p$.*

Since $a_0 + a_1 \cdot 0 + \ldots + a_{p-1} \cdot 0 \in B$ means $a_0 \in B$, it will be sufficient to show that

$$a_1 x + a_2 x^2 + \ldots + a_{p-1} x^{p-1} \in B \quad \text{for all } x \in Z_p$$

imply $a_1, \ldots, a_{p-1} \in B$.

Now

$$\begin{aligned} a_1 \cdot 1 + a_2 \cdot 1^2 \quad &+ \ldots + a_{p-1} \cdot 1^{p-1} &= b_1, \\ a_1 \cdot 2 + a_2 \cdot 2^2 \quad &+ \ldots + a_{p-1} \cdot 2^{p-1} &= b_2, \\ a_1 \cdot (p-1) + a_2 \cdot (p-1)^2 &+ \ldots + a_{p-1} (p-1)^{p-1} &= b_{p-1}, \end{aligned}$$

where $b_1, \ldots, b_{p-1} \in B$.

A is a vector space over Z_p and B is a subspace of A. The matrix of coefficients of $a_1, \ldots, a_{p-1}$ is non-singular and hence $a_1, \ldots, a_{p-1}$ are linear combinations of $b_1, \ldots, b_{p-1}$ and hence belong to B.

LEMMA 2. *Let A be a p-ring and B its subring. If $a_i \in A$ for all $i \in Z_p^n$ and $\sum \{a_i x^i : i \in Z_p^n\} \in B$ for all $x \in Z_p^n$, then $a_i \in B$ for all $i \in Z_p^n$.*

The proof will be by induction on n. The case $n = 1$ is Lemma 1. Let $m > 1$ and suppose Lemma 2 be true for all $1 \leqslant n < m$. Let $c \in Z_p^{m-1}$ and

$$\sum \{a_i x^i : i \in Z_p^m\} \in B \quad \text{for all } x \in Z_p^m.$$

In particular

$$\sum\{a_i, y^i\colon i\in Z_p^m\}\in B \quad \text{for } y_k = c_k,\ 1\leqslant k\leqslant m-1,$$

and for all $y_m\in Z_p$.

Thus $\sum\{b_i z^i\colon i\in Z_p\}\in B$ for all $z\in Z_p$, where $b_k = \sum\{a_i c^j\colon i_n = k, j_s = i_s,\ 1\leqslant s\leqslant m-1\}\in A$ for all $k\in Z_p$.

By Lemma 1, $b_k\in B$ for all $k\in Z_p$ and $c\in Z_p^{m-1}$.

By the induction hypothesis, Lemma 2 follows.

COROLLARY 4. *If A is a p-ring and $a_i\in A$ for all $i\in Z_p^n$, then $\sum\{a_i x^i\colon i\in Z_p^n\} = 0$ for all $x\in Z_p^n$, iff $a_i = 0$ for all $i\in Z_p^n$.*

Corollary 4 follows from Lemma 2 if we put $B = (0)$.

COROLLARY 5. *Let A be a p-ring and $a_i, b_i\in A$, for all $i\in Z_p^n$. Then $\sum\{a_i x^i\colon i\in Z_p^n\} = \sum\{b_i x^i\colon i\in Z_p^n\}$ for all $x\in Z_p^n$ iff $a_i = b_i$ for all $i\in Z_p^n$.*

This follows from Corollary 4 if we consider the difference between the expressions.

LEMMA 3. *Let A be a p-ring, $f\colon Z_p^n\to A$. Then there is a unique algebraic function $g\colon A^n\to A$ on A such that $f(x) = g(x)$ for all $x\in Z_p^n$.*

Proof. The uniqueness follows from Corollary 5.

To prove the existence of g, consider the system of equations

$$\sum\{a_i x^i\colon i\in Z_p^n\} = f(x)\in A, \qquad x\in Z_p^n.$$

In case $n = 1$, this is a system of p linear equations in p unknowns which can be reduced to a system of $p-1$ equations in $p-1$ unknowns whose matrix of coefficients is non-singular (like the proof of Lemma 1) and hence the unknowns $a_0, a_1, \ldots, a_{p-1}$ are linear combinations in $f(0), f(1), \ldots, f(p-1)$ which proves the existence for the case $n = 1$. The general case can be proved by induction and is similar to Lemma 2.

COROLLARY 6. *Let A be a p-ring with 1, then every function from Z_p^n into A can be extended uniquely to an algebraic function on A.*

COROLLARY 7. *Every function $f\colon Z_p^n\to Z_p$ is algebraic on Z_p. This is the well-known property that Z_p is primal.*

LEMMA 4. *Let A be a subdirect I-th power of Z_p. If $f\colon A^n\to A$ has the substitution property on A, then f is the restriction to A of*

$$\pi\{f_i\colon i\in I\}, \qquad \textit{where } f_i\colon Z_p^n\to Z_p,\ i\in I.$$

Proof. Let π_i denote the i-th projection of A onto Z_p and let $J_i = \pi_i^{-1}(0)$. J_i is an ideal of A. Let $i\in I$ be fixed and $a_1, \ldots, a_n, b_1, \ldots, b_n\in A$ such that $a_k(i) = b_k(i)$ for all $1\leqslant k\leqslant n$, i.e. $a_k - b_k\in J_i$ for all $1\leqslant k\leqslant n$.

Since f has the substitution property on A, we have $f(a_1, \ldots, a_n)(i) = f(b_1, \ldots, b_n)(i)$. Let $x_1, \ldots, x_n\in Z_p$ and choose $a_k\in\pi_i^{-1}(x_k)$, $1\leqslant k\leqslant n$.

Define $f_i\colon Z_p^n \to Z_p$ by

$$f_i(x_1, \ldots, x_n) = f(a_1, \ldots, a_n)(i).$$

It is clear that f_i does not depend on the choice of a_k in $\pi_i^{-1}(x_k)$, $1 \leqslant k \leqslant n$; moreover

$$f(a_1, \ldots, a_n)(i) = f_i\big(a_1(i), \ldots, a_n(i)\big),\ a_1, \ldots, a_n \in A.$$

COROLLARY 8. *Every function with the substitution property on $A = Z_p^I$ is algebraic on A.*

Let $f\colon A^n \to A$ be with the substitution property on A, then $f = \pi\{f_i\colon i \in I\}$ by Lemma 4. But every f_i is algebraic on Z_p, i.e.

$$f_i(x) = \sum \{k_{ij} x^j\colon j \in Z_p^n\}, \qquad x \in Z_p^n,$$

$$k_{ij} \in Z_p \quad \text{for all } j \in Z_p^n.$$

Define $a_j \in A$ by

$$a_j(i) = k_{ij}, \qquad i \in I;$$

for all $j \in Z_p^n$.

Then it is obvious that

$$f(x) = \sum \{a_j x^j\colon j \in Z_p^n\}, \qquad x \in A^n.$$

3. Now we are able to prove the Theorem.

Let A be a p-ring and $f\colon A^n \to A$ be a function with the substitution property on A. Then A is a subdirect I-th power of Z_p and, by Lemma 4, f is the restriction to A of $\pi\{f_i\colon i \in I\}$ where $f_i\colon Z_p^n \to Z_p$, $i \in I$. By Corollary 8 f is the restriction to A of an algebraic function on Z_p^I, i.e. there are elements $a_j \in Z_p^I$, $j \in Z_p^n$, such that

$$f(x) = \sum \{a_j x^j\colon j \in Z_p^n\}, \qquad x \in A^n.$$

If $x \in Z_p^n$, $b \in A$. Let xb denote $(x_1 b, \ldots, x_n b) \in A^n$. Then

$$\begin{aligned} f(xb) &= \sum \{a_j (xb)^j\colon j \in Z_p^n\} \\ &= \sum \{(a_j b^{j'}) x^j\colon j \in Z_p^n\} \in A \end{aligned}$$

for all $b \in A$, $x \in Z_p^n$, where

$$j' \in Z_p, \qquad j' = j_1 + j_2 + \ldots + j_n (\mathrm{mod}\, p).$$

By Lemma 2 $a_j b^{j'} \in A$ for all $j \in Z_p^n$ and all $b \in A$. Thus $a_j b = a_j b^{j'} \cdot b^{p-j'} \in A$ for all $b \in A$ and $j \in Z_p^n$, i.e. $a_j \in A^*$ for all $j \in Z_p^n$, i.e. f is the restriction to A of an algebraic function on A^*.

Conversely, let f be the restriction to A of an algebraic function g on A^*. If B is an ideal of A, B is also an ideal of A^*. Since $a \in A^*$, $b \in B$

implies $ab^{p-1} \epsilon A$. Hence $ab = ab^{p-1}b \epsilon B$, and so f has the substitution property on A since algebraic functions on A^* have the substitution property on A^*. This concludes the proof of the Theorem.

4. To deduce Corollary 1 we need only show that, if every function with the substitution property on A is algebraic on A, then $A_1 = A^*$.

Let $a \epsilon A^*$ then $f(x) = ax$; $x \epsilon A$ is the restriction to A of the algebraic function ax on A^*, f has the substitution property on A. Let f be algebraic on A, i.e.

$$ax = f(x) = \sum \{a_j x^j \colon j \epsilon Z_p\},$$

$a_0 \epsilon A$, $a_j \epsilon A_1$ for all $x \epsilon A$.

$$(ax)(i) = f(x)(i) = \sum \{a_j(i)\big(x(i)\big)^j \colon j \epsilon Z_p\},$$

$i \epsilon I$ for all $x \epsilon A$.

Since A is a subdirect I-th power of Z_p, $x(i)$ takes all values of Z_p as x runs all over A. Thus

$$a(i)z = \sum \{a_j(i) z^j \colon j \epsilon Z_p\}$$

for all $z \epsilon Z_p$.

By Corollary 5

$$a(i) = a_1(i) \quad \text{for all } i \epsilon I,$$

i.e. $a = a_1 \epsilon A_1$ and hence $A^* \subseteq A_1$ which concludes the proof of Corollary 1.

Now we construct an example of a p-ring A such that not every function with the substitution property on A is algebraic.

Let A be the direct sum of N copies of Z_p where N is the set of natural numbers $\{1, 2, \ldots\}$. Define $c \epsilon Z_p^N$ by

$$c(2n) = 0, \quad c(2n+1) = 1.$$

It is clear that A is an ideal of Z_p^N and so $A^* = Z_p^N$, however $c \notin A_1$ i.e. $A_1 \neq A^*$. The function $f(x) = cx$ enjoys the substitution property on A but it is not algebraic on A.

REFERENCES

[1] G. Grätzer, *Universal algebra*, New York 1968.

[2] — *On Boolean functions (Notices on lattice theory II)*, Revue de Mathématiques Pures et Appliquées 7 (1962), p. 693-697.

[3] — *Boolean functions on distributive lattices*, Acta Mathematica Academiae Scientiarum Hungaricae 15 (1964), p. 195-201.

[4] N. H. McCoy and Deane Montgomery, *A representation of generalized Boolean rings*, Duke Mathematical Journal 3 (1937), p. 456-459.

VANDERBILT UNIVERSITY
NASHVILLE, TENNESSEE, USA

Reçu par la Rédaction le 8. 11. 1970