PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 29, No. 2, July 1971

THE CATEGORIES OF p-RINGS ARE EQUIVALENT

R. W. STRINGALL

ABSTRACT. Let p and q be prime numbers. Let R_p and R_q denote, respectively, the categories of p-rings and q-rings with ring homomorphisms as morphisms. Then R_p and R_q are equivalent categories. In particular, the category of all Boolean rings is equivalent to R_p.

Stone, in [5], remarked on the now verified close connection between the representation of Boolean rings and direct decompositions of rings. Using some elementary properties of radical rings, Theorem 5.10 of [7] and the result mentioned in the abstract, it is easily shown that there is a useful extension of Stone's connection to the study of decompositions of Abelian p-groups (see [6]). Moreover, if a theorem of R. S. Pierce [4, 14.3] is considered, then it can be seen that this extended connection has general application to the structure problem of Abelian p-groups. In addition, interest in the representation theorem of this note lies in the connection between p-rings and the theories of Stone, Carathéodory and Boole and Whitehead.

Let p be a prime number. A nontrivial commutative, associative ring R is called a *p-ring or generalized Boolean ring* if it satisfies the identities $x^p = x$ and $px = 0$. If $p = 2$, then R is called a *Boolean ring*.

Stone [5] has demonstrated that every Boolean ring is isomorphic to a ring of subsets of some set. McCoy and Montgomery [2] point out that this result is equivalent to the theorem that every Boolean ring is isomorphic to a subring of a direct sum of rings F_2 (F_p denotes the prime field of characteristic p). Moreover, they prove, using methods similar to those employed by Stone, Alexander and Zippin, that this result generalizes to the theorem that every p-ring is isomorphic to a subring of a direct sum of fields F_p. Clearly, every subdirect sum of fields F_p is a p-ring and this result is, consequently, a "complete characterization" of p-rings.

The direction of this note will be to assume the above characterization of p-rings and then to show, using this setting, that the categories R_p and R_2 are equivalent.

Received by the editors March 24, 1970 and, in revised form, September 15, 1970.

AMS 1970 *subject classifications*. Primary 06A40, 16A00, 16A32; Secondary 02J05, 20K25.

Key words and phrases. Category of Boolean rings, category of p-rings, subdirect sums of finite fields, p-rings, Boolean rings, Abelian p-groups, decompositions of Abelian p-groups, Boolean rings of idempotents.

Let R be any subring of $\prod_{\gamma\in\Gamma} R_\gamma$ where $R_\gamma \cong F_p\ \forall\gamma\in\Gamma$. Let π_γ be the natural projection of R onto R_γ and denote the identity of R_γ by 1_γ. For each subset $A\subseteq\Gamma$, define $\sigma(A)\in\prod_{\gamma\in\Gamma} R_\gamma$ by

$$\begin{aligned}\pi_\gamma\sigma(A) &= 1_\gamma \qquad \text{if } \gamma\in A,\\ &= 0 \qquad \text{if } \gamma\notin A.\end{aligned}$$

Clearly, if $r\in\prod R_\gamma$ and if $A_i(r)=\{\gamma\in\Gamma:\pi_\gamma r=i\cdot 1_\gamma\}$ for each $i=0, 1,\cdots, p-1$; then r can be written uniquely in the form $r=\sum_{i=0}^{p-1} i\sigma(A_i(r))$.

Results similar to the following proposition can be found in papers by Foster [1] and Zemmer [8].

PROPOSITION 1. *Let* $R\subset\prod_{\gamma\in\Gamma} R_\gamma$, $r\in R$ *and* $r=\sum_{i=0}^{p-1} i\sigma(A_i(r))$. *Then* $\bigcup_{i=0}^{p-1} A_i(r)=\Gamma$, $A_i(r)\cap A_j(r)=\varnothing$ *if* $i\neq j$ *and* $\sigma(A_i(r))\in R$ *if* $i\neq 0$.

PROOF. It is first noted that while R may not have an identity it is possible to find a subring S of R with identity which contains r. The identities $r^{p-1}r=r^p=r$ and $r^{p-1}(r^{p-1}s)=r^{p-1}s$ for all $s\in R$ imply that $r^{p-1}R=S$ is such a subring. Moreover if e is the identity of S, then, clearly, $e=r^{p-1}$. For $k\neq 0$, consider the product

$$s=\prod_{i\neq k;\, i=0,1,\cdots,p-1}(ie-r)\in S.$$

It will be shown that $s=-\sigma(A_k(r))$. Suppose $\gamma\notin A_k(r)$, then $\pi_\gamma(s)=0$ since $\gamma\in A_i(r)$ for some $i\neq k$. Moreover, an application of Fermat's theorem yields $\pi_\gamma(ie-r)=\pi_\gamma ir^{p-1}-\pi_\gamma r=i(\pi_\gamma r)^{p-1}-\pi_\gamma r=i1_\gamma-i1_\gamma=0$. If $\gamma\in A_k(r)$, then

$$\begin{aligned}\pi_\gamma s &= \prod_{i\neq k;\, i=0,1,\cdots,p-1}(\pi_\gamma(ie-r)) = \prod_{i\neq k;\, i=0,1,\cdots,p-1}(i(\pi_\gamma r)^{p-1}-\pi_\gamma r)\\ &= \prod_{i\neq k;\, i=0,1,\cdots,p-1}(i\cdot 1_\gamma - k\cdot 1_\gamma)\\ &= 1_\gamma\cdot[(0-k)(1-k)(2-k)\cdots((k-1)-k)\\ &\qquad\cdot((k+1)-k)\cdots((p-1)-k)]\\ &= 1_\gamma\cdot(p-1)!.\end{aligned}$$

Now by Wilson's theorem $(p-1)!\equiv -1$ (modulo p). Hence, $\sigma(A_k(r)) = -s\in S\subseteq R$. The remainder of the result is obvious.

It is known that if S is any associative ring and if $I(S)$ represents the collection of all central idempotents in S, then $I(S)$ can be made into a Boolean ring, $\langle I(S),\oplus,\cdot\rangle$, by defining $e\oplus f=e+f-2ef$ and

$e\cdot f=ef$ for all e, $f\in I(S)$. The following proposition gives a more descriptive representation of $I(R)$ for the p-ring R.

PROPOSITION 2. *Let $R\subseteq\prod_{\gamma\in\Gamma}R_\gamma$ and let $K(R)=\{A\subseteq\Gamma:\sigma(A)\in R\}$. Then $K(R)$ together with the operations $A+B=(A\cup B)-(A\cap B)$ and $A\cdot B=A\cap B$ forms a Boolean ring of subsets of Γ. Moreover, $I(R)=\sigma(K(R))$ and the correspondence $A\leftrightarrow\sigma(A)$ is an isomorphism between the Boolean rings $K(R)$ and $I(R)$.*

PROOF. An application of Fermat's theorem yields for each $r=r^2\in R$, $r=r^{p-1}=\sigma(A)$ where $A=\{\gamma\in\Gamma:\pi_\gamma r\neq 0\}$. Conversely, if $A\in K(R)$, then $\sigma(A)\in I(R)$. Hence $I(R)=\{\sigma(A):A\in K(R)\}$. It follows that σ is one-to-one and onto $I(R)$. That $K(R)$ is a Boolean ring and σ an isomorphism follows by standard arguments using the identities:

$$\sigma(A\cdot B)=\sigma(A\cap B)=\sigma(A)\cdot\sigma(B)$$

and

$$\begin{aligned}\sigma(A+B)&=\sigma(A\cup B-A\cap B)=\sigma(A)+\sigma(B)-2\sigma(A)\sigma(B)\\&=\sigma(A)\oplus\sigma(B).\end{aligned}$$

Let $\mathcal{B}$ be any Boolean ring of subsets of Γ. The set $\{\sigma(A):A\in\mathcal{B}\}$ generates a subring of $\prod_{\gamma\in\Gamma}R_\gamma$. Denote this subring by $\mathcal{L}(\mathcal{B})$. The following corollary to Propositions 1 and 2 is now apparent.

COROLLARY 1. *If R is a subring of $\prod_{\gamma\in\Gamma}R_\gamma$, then $\mathcal{L}(K(R))=R$. Moreover, if $\mathcal{B}$ is any Boolean ring of subsets of Γ, then $\mathcal{B}=K(\mathcal{L}(\mathcal{B}))$.*

With the aid of the Stone representation theorem for Boolean rings:

COROLLARY 2. *If p is prime, then every Boolean ring is isomorphic to the Boolean ring of idempotents of some p-ring.*

PROOF. Let $\mathcal{B}$ be a Boolean ring. Then by Stone's theorem, $\mathcal{B}$ is isomorphic to a ring of subsets of some set Γ. Thus, $\mathcal{L}(\mathcal{B})\subset\prod_{\gamma\in\Gamma}R_\gamma$ is a p-ring which, by Proposition 2 and Corollary 1, contains the desired isomorphic copy of $\mathcal{B}$.

THEOREM 1. *Let R, S be p-rings and $I(R)$, $I(S)$ the corresponding Boolean rings.* (i) *Every homomorphism $R\to S$ restricts to a Boolean homomorphism $I(R)\to I(S)$.* (ii) *Every Boolean homomorphism $I(R)\to I(S)$ is the restriction of a unique ring homomorphism $R\to S$.*

PROOF. It may be assumed that R and S are subrings of $\prod_{\gamma\in\Gamma}R_\gamma$ for some Γ.

(i) If $h:R\to S$ is any ring homomorphism, then for e_1, $e_2\in I(R)$,

$$h(e_1\cdot e_2)=h(e_1)h(e_2)$$

and

$$h(e_1 \oplus e_2) = h(e_1 + e_2 - 2e_1e_2) = h(e_1) + h(e_2) - 2h(e_1)h(e_2)$$
$$= h(e_1) \oplus h(e_2).$$

(ii) Clearly, by Proposition 1 there can exist at most one homomorphism $R \to S$ which restricts to a given Boolean homomorphism $I(R) \to I(S)$. Let $g: I(R) \to I(S)$ be a Boolean homomorphism. For $r = \sum_{i=0}^{p-1} i\sigma(A_i(r)) \in R$, define $h(r) = \sum_{i=1}^{p-1} ig(\sigma(A_i(r)))$. The map h is well defined since the representation $r = \sum_{i=0}^{p-1} i\sigma(A_i(r))$ is unique. Moreover, h agrees with g on $I(R)$. To complete the proof of (ii), it is only necessary to show that h is a ring homomorphism. To do this three items are first noted:

(1) If $r, s \in R$ and if $0 < i_0 < p$, then $A_0(r) \cap A_{i_0}(s) \in K(R)$ and hence $\sigma(A_0(r) \cap A_{i_0}(s)) \in R$. This is immediate from Proposition 1 and the fact that Boolean rings are closed with respect to relative complementation. For if $r, s \in R$ and $i_0 \neq 0$, then $A_{i_0}(s) \in K(R)$, $A_i(r) \in K(R)$ for all $i \neq 0$, $A_i(r) \cap A_j(r) = \varnothing$ for $i \neq j$ and $\bigcup_{i=0}^{p-1} A_i(r) = \Gamma$. It follows that $\bigcup_{i \neq 0} A_i(r) \in K(R)$ and $A_{i_0}(s) \cap A_0(r) = A_{i_0}(s) - \bigcup_{i \neq 0} A_i(r) \in K(R)$.

(2) Suppose $A_1, A_2, \cdots, A_n \in K(R)$ are disjoint, a_i is an integer for $i = 1, 2, \cdots, n$ and $r = \sum_{i=1}^{n} a_i\sigma(A_i)$. Then $\sum_{i=1}^{n} a_ih(\sigma(A_i)) = \sum_{k=1}^{p-1} kh(\sigma(A_k(r))) = h(r)$. To prove this, first note that $\sigma^{-1}h\sigma(A_1)$, $\sigma^{-1}h\sigma(A_2), \cdots, \sigma^{-1}h\sigma(A_n) \in K(S)$ are disjoint since, if $i \neq j$ and $\sigma^{-1}h\sigma(A_i) \cap \sigma^{-1}h\sigma(A_j) \neq \varnothing$, then $0 \neq h\sigma(A_i) \cdot h\sigma(A_j) = h(\sigma(A_i)\sigma(A_j)) = h(\sigma(A_i \cap A_j)) = h(0)$, a contradiction. Since, in addition to $A_1, \cdots, A_n$ forming a disjoint collection

$$A_k(r) = \bigcup\{A_i : a_i \equiv k \pmod{p}\} \quad \text{for } k = 1, \cdots, p-1,$$

it follows that

$$h(\sigma(A_k(r))) = \sum_{a_i \equiv k \pmod{p}} h(\sigma(A_i)).$$

Therefore, for $k \neq 0$,

$$kh(\sigma(A_k(r))) = \sum_{a_i \equiv k \pmod{p}} a_ih(\sigma(A_i))$$

and

$$h(r) = \sum_{k=1}^{p-1} kh(\sigma(A_k(r))) = \sum_{k=1}^{p-1} \sum_{a_i \equiv k \pmod{p}} a_ih(\sigma(A_i)) = \sum_{i=1}^{n} a_ih(\sigma(A_i)).$$

(3) If A and B are disjoint members of $K(R)$, then $h\sigma(A) \oplus h\sigma(B) = h\sigma(A) + h\sigma(B)$. This follows since $h = g$ on $I(R)$ and

$$\begin{aligned} g\sigma(A) \oplus g\sigma(B) &= g\sigma(A) + g\sigma(B) - 2(g\sigma(A))(g\sigma(B)) \\ &= g\sigma(A) + g\sigma(B) - 2g(\sigma(A)\cdot\sigma(B)) \\ &= g\sigma(A) + g\sigma(B) - 2g\sigma(A \cap B) \\ &= g\sigma(A) + g\sigma(B). \end{aligned}$$

Now suppose $r = \sum_{i=0}^{p-1} i\sigma(A_i(r))$ and $s = \sum_{i=0}^{p-1} i\sigma(A_i(s))$ are elements in R. Then, for each $\gamma \in \Gamma$,

$$\begin{aligned} \pi_\gamma(r+s) &= \pi_\gamma \sum_{i=0}^{p-1} i\sigma(A_i(r)) + \sum_{i=0}^{p-1} i\sigma(A_i(s)) \\ &= \pi_\gamma \sum_{i=0;\,j=0}^{p-1} (i+j)\sigma(A_i(r) \cap A_j(s)). \end{aligned}$$

Hence

$$r + s = \sum_{i=0;\,j=0}^{p-1} (i+j)\sigma(A_i(r) \cap A_j(s))$$

and by (1) the sets $A_i(r) \cap A_j(s)$ are disjoint members of $K(R)$ provided i and j are not both zero. Thus, by (2),

$$h(r+s) = \sum_{i,j;\,i+j\neq 0}^{p-1} (i+j)h(\sigma(A_i(r) \cap A_j(s))).$$

Now, $\bigcup_{i=0}^{p-1} A_i(s) = \Gamma$ and the sets $A_i(r) \cap A_j(s)$ are disjoint. Moreover, $A_i(r) \cap A_j(s) \in K(R)$ if one, i or j is not zero. Thus for $i \neq 0$,

$$h\sigma(A_i(r)) = h\sigma\left(\bigcup_{j=0}^{p-1} (A_i(r) \cap A_j(s))\right) = h\sigma\left(\sum_{j=0}^{p-1} (A_i(r) \cap A_j(s))\right)$$

where the latter sum is that in $K(R)$, (see Proposition 2). Continuing,

$$\begin{aligned} h\sigma(A_i(r)) &= h(\sigma(A_i(r) \cap A_0(s)) \\ &\quad \oplus \sigma(A_i(r) \cap A_1(s)) \oplus \cdots \oplus \sigma(A_i(r) \cap A_{p-1}(s))) \end{aligned}$$

since σ is an isomorphism of $K(R)$ onto $I(R)$. Moreover, using the fact that h restricted to $I(R)$ is a Boolean homomorphism and applying (3),

$$\begin{aligned} h\sigma(A_i(r)) &= h\sigma(A_i(r) \cap A_0(s)) \\ &\quad \oplus h\sigma(A_i(r) \cap A_1(s)) \oplus \cdots \oplus h\sigma(A_i(r) \cap A_{p-1}(s)) \\ &= \sum_{j=0}^{p-1} h\sigma(A_i(r) \cap A_j(s)). \end{aligned}$$

Thus,

$$h(r) = \sum_{i=1}^{p-1} ih(\sigma(A_i(r))) = \sum_{i=1}^{p-1}\sum_{j=0}^{p-1} ih\sigma(A_i(r) \cap A_j(s)).$$

Similarly,

$$h(s) = \sum_{j=1}^{p-1} jh(\sigma(A_j(s))) = \sum_{j=1}^{p-1}\sum_{i=0}^{p-1} jh\sigma(A_i(r) \cap A_j(s))$$

it follows that $h(r+s) = h(r) + h(s)$.

To show that $h(r)\cdot h(s) = h(rs)$, note that

$$\begin{aligned} rs &= \left(\sum_{i=1}^{p-1} i\sigma(A_i(r))\right)\cdot\left(\sum_{j=1}^{p-1} j\sigma(A_j(s))\right) \\ &= \sum_{i=1}^{p-1}\sum_{j=1}^{p-1} ij\sigma(A_i(r) \cap A_j(s)) \end{aligned}$$

and

$$h(rs) = \sum_{i=1}^{p-1}\sum_{j=1}^{p-1} ijh\sigma(A_i(r) \cap A_j(s)) \quad \text{by (2).}$$

On the other hand,

$$\begin{aligned} h(r)h(s) &= \left(\sum_{i=1}^{p-1} ih\sigma(A_i(r))\right)\left(\sum_{j=1}^{p-1} jh\sigma(A_j(s))\right) \\ &= \sum_{i=1}^{p-1}\sum_{j=1}^{p-1} ijh(\sigma(A_i(r)))h(\sigma(A_j(s))) \\ &= \sum_{i=1}^{p-1}\sum_{j=1}^{p-1} ijh(\sigma(A_i(r))\sigma(A_j(s))) \\ &= \sum_{i=1}^{p-1}\sum_{j=1}^{p-1} ijh(\sigma(A_i(r) \cap A_j(s))). \end{aligned}$$

Hence, $h(r)\cdot h(s) = h(rs)$.

The proof of the following corollary follows from the observation that the correspondence $R \to I(R)$ together with the restriction map $g \to g \restriction I(R)$ is a full, representative, faithful functor from the category of all p-rings to the category of all Boolean rings [3].

COROLLARY 3. *If p and q are prime members, then the categories R_p and R_q are equivalent.*

BIBLIOGRAPHY

1. A. L. Foster, *p-rings and their Boolean-vector representation*, Acta. Math. **84** (1951), 231–261. MR **12**, 584.

2. N. H. McCoy and D. Montgomery, *A representation of generalized Boolean rings*, Duke Math. J. **3** (1937), 455–459.

3. B. Mitchell, *Theory of categories*, Pure and Appl. Math., vol. **17**, Academic Press, New York, 1965. MR **34** #2647.

4. R. S. Pierce, *Homomorphisms of primary Abelian groups*, Proc. Sympos. Topics in Abelian Groups (New Mexico State University, 1962), Scott, Foresman, Chicago, Ill., 1963, pp. 215–310. MR **31** #1299.

5. M. H. Stone, *The theory of representations for Boolean algebras*, Trans. Amer. Math. Soc. **40** (1936), 37–111.

6. R. W. Stringall, *Decompositions of Abelian p-groups*, Proc. Amer. Math. Soc. **28** (1971), 409–410.

7. ———, *Endomorphism rings of primary Abelian groups*, Pacific J. Math. **20** (1967), 535–557. MR **34** #7644.

8. J. L. Zemmer, *Some remarks on p-rings and their Boolean geometry*, Pacific J. Math. **6** (1956), 193–208. MR **18**, 108.

UNIVERSITY OF CALIFORNIA, DAVIS, CALIFORNIA 95616