COLLOQUIUM MATHEMATICUM

VOL. XXVII 1973 FASC. 2

ON THE ARITY OF IDEMPOTENT REDUCT OF ABELIAN GROUPS

BY

J. PŁONKA (WROCŁAW)

Let $\mathfrak{A} = (X, F)$ be a universal algebra. Let us denote by $A(F)$ the family of all polynomials in $\mathfrak{A}$. We identify two algebras $\mathfrak{A} = (X, F)$ and $\mathfrak{B} = (X, G)$ if $A(G) = A(F)$, and we write $\mathfrak{A} = \mathfrak{B}$. We say that $\mathfrak{B}$ is a *reduct* of an algebra $\mathfrak{A}$ if $\mathfrak{A} = (X, F)$, $\mathfrak{B} = (X, G)$ and $A(G) \subseteq A(F)$. Denote by $A^{(n)}(F)$ the family of all n-ary polynomials in $\mathfrak{A}$. A polynomial $f(x_1, \ldots, x_n)$ is called *symmetrical* if, for any permutation ν of the indices $1, \ldots, n$, we have $f(x_1, \ldots, x_n) = f(x_{\nu(1)}, \ldots, x_{\nu(n)})$. Let us denote by $A_s^{(n)}(F)$ the family of all symmetrical n-ary operations.

For a given algebra $\mathfrak{A} = (X, F)$ E. Marczewski defined two numbers $\varrho(\mathfrak{A})$ and $\varrho_s(\mathfrak{A})$ as follows:

$$\varrho(\mathfrak{A}) := \min\{n \mid \mathfrak{A} = (X, A^{(n)}(F))\},$$

$$\varrho_s(\mathfrak{A}) := \min\{n \mid \mathfrak{A} = (X, \bigcup_{j=0}^{n} A_s^{(j)}(F))\}.$$

We call $\varrho(\mathfrak{A})$ the *arity*, and $\varrho_s(\mathfrak{A})$ the *symmetrical arity* of $\mathfrak{A}$. An algebra $\mathfrak{A} = (X, F)$ is called *symmetrical* if $\mathfrak{A} = (X, S)$, where $S \subseteq A(F)$, and all operations of S are symmetrical.

A polynomial $f(x_1, \ldots, x_n)$ is called *idempotent* if $f(x, \ldots, x) = x$. For a given algebra $\mathfrak{A} = (X, F)$ we denote by $\mathfrak{I}(\mathfrak{A})$ the algebra $(X, I(F))$, where $I(F)$ is the set of all idempotent polynomials in $\mathfrak{A}$. The algebra $\mathfrak{I}(\mathfrak{A})$ is called the *idempotent reduct* of the algebra $\mathfrak{A}$.

THEOREM 1. *Let $\mathfrak{G} = (G, \cdot)$ be an Abelian group satisfying $x^m = 1$, $m > 1$, and let p be a prime not dividing m. Then $\mathfrak{I}(\mathfrak{G}) = (G, x_1^n \cdot \ldots \cdot x_p^n)$, where n is the number such that $n < m$ and $np \equiv 1\ (m)$, and $\mathfrak{I}(\mathfrak{G})$ is a symmetrical algebra.*

Proof. It is clear that there exists an n such that $np \equiv 1(m)$, and that, by Euler's theorem, there is a number k such that $n^k \equiv 1(m)$. Put

$$f(x_1, \ldots, x_p) = x_1^n \ldots x_p^n \quad \text{and} \quad r(x, y) = f(x, y, \ldots, y).$$

Then

$$f\Big(\underbrace{r\big(r\big(\ldots r\big(}_{k-1\text{ times}}r(x,z),z\big),\ldots,z\big),z\big),\underbrace{r\big(r\big(\ldots r\big(}_{k-1\text{ times}}r(y,z),z\big),\ldots,z\big),z\big),\underbrace{z,\ldots,z}_{p-2\text{ times}}\Big)$$

is equal to $xyz^{m-1} = xyz^{-1}$ which, by Theorem 1 of one of my papers (1), generates every polynomial in $\mathfrak{J}(\mathfrak{G})$.

THEOREM 2. *Let $\mathfrak{G}$ be an Abelian group satisfying $x^m = 1$ for a minimal $m > 1$, and let p be the smallest prime not dividing m. If $1 < q < p$, then there is no symmetrical q-ary operation in $A\big(\mathfrak{J}(\mathfrak{G})\big)$, and so $\varrho_s\big(\mathfrak{J}(\mathfrak{G})\big) = p$.*

Proof. From assumption it follows that $(m, q) \neq 1$, whence $qs \not\equiv 1 (m)$ for every s. Consequently, the operation $x_1^s \ldots x_q^s$ cannot be in $A\big(\mathfrak{J}(\mathfrak{G})\big)$. This, in virtue of Theorem 1, implies $\varrho_s\big(\mathfrak{J}(\mathfrak{G})\big) = p$.

COROLLARY. *For any prime $p > 2$ there exists an idempotent algebra $\mathfrak{A}$ with $\varrho(\mathfrak{A}) = 3$ and $\varrho_s(\mathfrak{A}) = p$.*

In fact, it suffices to put $\mathfrak{A} = \mathfrak{J}(Z_{(p-1)!})$ (Z_k means cyclic group of order k) and to apply Theorem 2 and the results of my above-cited paper.

One can ask whether for given two numbers m and n such that $1 < n < m$ there exists an algebra $\mathfrak{A}$ with $\varrho_s(\mathfrak{A}) = m$, $\varrho(\mathfrak{A}) = n$. (**P 829**)

(1) J. Płonka, *On the arity of idempotent reducts of groups*, Colloquium Mathematicum 21 (1970), p. 35-37.

Reçu par la Rédaction le 14. 1. 1972