COLLOQUIUM MATHEMATICUM

VOL. XXI 1970 FASC. 1

ON THE ARITY OF IDEMPOTENT REDUCTS OF GROUPS

BY

J. PŁONKA (WROCŁAW)

0. For a given algebra $\mathfrak{A} = (A; F)$ we shall denote by $A(F)$ the family of its all algebraic operations, and by $A^{(n)}(F)$ the family of its all n-ary algebraic operations. In the sequel we shall not distinguish algebras with the same set $A(F)$. E. Marczewski defined the arity $\varrho(\mathfrak{A})$ of an algebra $\mathfrak{A} = (A; F)$ as follows:

$$\varrho(\mathfrak{A}) = \min\{n: (A; F) = (A; A^{(n)}(F))\}.$$

The number ϱ has been studied by K. Urbanik (1).

An operation $f(x_1, \ldots, x_n)$ is called *idempotent* if $f(x, x, \ldots, x) = x$. For a given algebra $\mathfrak{A} = (A; F)$ let $\mathfrak{I}(\mathfrak{A})$ be the algebra $(A; I(F))$, where $I(F)$ denotes the family of all idempotent algebraic operations of the algebra $\mathfrak{A}$. We shall call $\mathfrak{I}(\mathfrak{A})$ the *idempotent reduct* of $\mathfrak{A}$. In this note we shall investigate the arity of idempotent reducts of groups.

1. Let $G = (G; \cdot, ^{-1})$ be a group. The following two observations are obvious:

(i) Every algebraic operation in G can be written in the form $x_{i_1}^{\delta_1} \ldots x_{i_n}^{\delta_n}$, where $\delta_k = \pm 1$, and for every k either $i_k \neq i_{k+1}$ or $\delta_k \neq \delta_{k+1}$.

(ii) An operation of the form given in (i) is idempotent if and only if the number of exponents δ_k equal to $+1$ equals $p+1$ with $n = 2p+1$.

Let us define $f(x, y, z) = x^{-1}yz$, $g(x, y, z) = xy^{-1}z$, $h(x, y, z) = xyz^{-1}$.

LEMMA 1. *For every group G we have $\mathfrak{I}(G) = (G; f, h)$.*

Proof. We have to show that the operations f and h generate all idempotent operations of G. We shall do it by induction with respect to the number p occurring in (ii). For $p = 0$ and $p = 1$ this is trivial. Assume now that every algebraic idempotent operation with $p = m-1$ is generated by f and h, and let $s(x_1, \ldots, x_n)$ be an idempotent algebraic operation with $p = m$, $n = 2m+1$. There must exist then an index k with

(1) K. Urbanik, *On some numerical constants associated with abstract algebras, II*, Fundamenta Mathematicae 52 (1968), p. 191–210.

$1 \leqslant k \leqslant 2p-1$ and such that $x_{i_k}^{\delta_k} \cdot x_{i_{k+1}}^{\delta_{k+1}} \cdot x_{i_{k+2}}^{\delta_{k+2}}$ is equal to f, g or h, because otherwise every two variables with positive exponents would be separated by at least two variables with negative exponents and so the number of variables with negative exponents occurring in $s(x_1, \ldots, x_n)$ would exceed $2p$, contrary to (ii). Let us denote $x_{i_k}^{\delta_k} x_{i_{k+1}}^{\delta_{k+1}} x_{i_{k+2}}^{\delta_{k+2}}$ by u^1. We obtain a word s which is idempotent and in which the number of positive exponents equals $p-1$. In view of our induction assumption this word is a superposition of f and h; but u^1 is equal to f, g or h, and so by (i) the word s can be written as the superposition of f and h.

As a corollary the following result follows:

THEOREM I. *For every group G we have $\varrho(\mathfrak{I}(G)) \leqslant 3$.*

Now we prove

THEOREM II. *For a free group G we have $\varrho(\mathfrak{I}(G)) = 3$.*

Proof. Observe that in any free group of the class defined by $X^2 = 1$ there are no non-trivial binary idempotent operations, and so for those groups the equality $\varrho(\mathfrak{I}(G)) = 3$ holds. Clearly, this implies that the last equality holds for any free group.

LEMMA 2. *To each natural number n there corresponds a natural number k_0 such that the following congruence holds:*

$$\frac{(n+1)[(n+1)^{k_0}-1]}{n} \equiv 2n \pmod{2n+1}.$$

Proof. Take $k_0 = \varphi(2n+1)-1$. Then, by Euler's theorem, we have

$$(n+1)^{k_0+1} \equiv 1 \pmod{2n+1},$$

and so

$$\begin{aligned}\frac{(n+1)[(n+1)^{k_0}-1}{n} - 2n &\equiv \frac{(n+1)[(n+1)^{k_0}-1]}{n} + 1 \\ &= \frac{(n+1)[(n+1)^{k_0}-1]+n}{n} = \frac{(n+1)^{k_0+1}}{n} - 1 \\ &\equiv 0 \pmod{2n+1}.\end{aligned}$$

LEMMA 3. *If G is an abelian group in which the identity $x^{2n+1} = 1$ is satisfied, then $\mathfrak{I}(G)$ is a groupoid $(G; f(x, y))$, where $f(x, y) = x^{n+1}y^{n+1}$.*

Proof. Let $f_0(x, y) = f(x, y)$ and $f_{k+1}(x, y) = f(x, f_{k-1}(x, y))$. It easy to see that the variable x occurs in $f_k(x, y)$ with the exponent $(n+1)[(n+1)^k-1]/n$, and so, in view of Lemma 2, we shall have for some k_0 the equality $f_{k_0}(x, y) = x^{2n}y^2$. Moreover, we have $f_k(x, f(y, z)) = x^{2n}y^{2n+2}z^{2n+2} = x^{-1}yz = f(x, y, z)$, where f is defined as in Lemma 1. Since our group is abelian, we have $h(x, y, z) = f(z, x, y)$, and so it follows

from Lemma 1 that every idempotent algebraic operation in G can be represented as a superposition of $f(x, y)$.

From this lemma we get the following

THEOREM III. *If G is an abelian group satisfying $x^{2n+1} = 1$, then $\varrho(\mathfrak{I}(G)) = 2$.*

Finally, we prove

THEOREM IV. *Let G be an abelian group satisfying $x^{2n} = 1$ but not satisfying any identity of the form $x^{2m+1} = 1$. Then we have $\varrho(\mathfrak{I}(G)) = 3$. Similarly, if Z is the cyclic infinite group, then $\varrho(\mathfrak{I}(Z)) = 3$.*

Proof. It suffices to prove the first part, as the second will follow. Observe that every idempotent algebraic operation in an abelian group satisfying the condition $x^{2n} = 1$, where n is chosen as small as possible, has the form $x^k y^m$ with $k+m = 2n+1$. It is clear that exactly one of the numbers k and m must be even. Superposing such operations, we obtain operations in which at least one exponent is even. But the idempotent algebraic operation $f(x, y, z) = x^{2n-1}yz$ has all its exponents odd, and so it cannot be generated by binary idempotents. This proves the theorem.

INSTITUTE OF MATHEMATICS OF THE POLISH ACADEMY OF SCIENCES

Reçu par la Rédaction le 24. 10. 1968