On group operations other than xy or yx

By A. HULANICKI (Wrocław) and S. ŚWIERCZKOWSKI (Glasgow)

1. Introduction. Professor E. MARCZEWSKI suggested recently a notion of *weak isomorphism* of algebraic systems (see „Definition" below). In this paper we solve a problem raised by him, concerning the weak isomorphism of groups.

In the course of the solution we show the existence of groups G which have the following

Property ($\ast$): There is a binary operation $x \circ y$ in G, other than xy or yx, i. e. a word

$$x \circ y = x^{k_1} y^{l_1} x^{k_2} y^{l_2} \dots x^{k_r} y^{l_r} \quad (k_i, l_i \text{ integers})$$

not identically equal in G to xy or to yx, such that

(i) the elements of G form a group $G_\circ$ under the operation $x \circ y$,

(ii) the operation xy is a word in $G_\circ$, i. e. there are integers $m_1, \dots, m_s$ and $n_1, \dots, n_s$ such that

$$xy = [x]_\circ^{m_1} \circ [y]_\circ^{n_1} \circ \dots \circ [x]_\circ^{m_s} \circ [y]_\circ^{n_s}$$

holds identically for all x, y in G ($[x]_\circ^m$ denotes the m-th power of x with respect to the multiplication $\circ$ in $G_\circ$).

G. HIGMAN and B. H. NEUMANN [1] have proposed the following problem: "Is there any binary operation in a group G, other than xy^{-1} or yx^{-1} and their transposes, in terms of which all group operations can be expressed?" Our examples of groups with Property ($\ast$) answer this question. For, it is clear that if G has Property ($\ast$), then $x \circ y^{(-1)}$ where by $y^{(-1)}$ we mean the inverse element of y with respect to the $\circ$ multiplication is an operation required by G. HIGMAN and B. H. NEUMANN.

As has been recently shown by HANNA NEUMANN [3], if G is a free group, then any binary operation in G which is associative is of one of the following types: a, x, y, xay, yax where a is any constant element of G. This covers an unpublished result of K. URBANIK that a free group does not possess Property ($\ast$). It follows from our Theorem 1 (see the Remark) that a free nilpotent group of class 2 does not possess Property ($\ast$) either.

We prove below that if G is a periodic nilpotent group of class 2 and G has Property ($\ast$), then the groups G and $G_\circ$ are isomorphic (Theorem 2). We do not know whether our assumptions are essential and we would like to suggest the following

PROBLEM. If G has Property $(\ast)$, are G and $G_\circ$ isomorphic?

We now proceed to define the notion of weak isomorphism of two algebraic systems. By an *algebraic system*, or shortly *algebra*, we mean a pair (A, F) composed of a set A and a family F of operations (functions) of finitely many variables defined on A and taking values in A. For every positive integer n we define the class $\mathbf{A}^{(n)}$ of *algebraic operations of n variables* as the smallest class of operations such that

(j) the identity operations $e_j^n(x_1, \ldots, x_n)$ defined by

$$e_j^n(x_1, \ldots, x_n) = x_j \text{ for all } x_1, \ldots, x_n,$$

belong to $\mathbf{A}^{(n)}$,

(jj) if $f \in F$ is an operation of m variables and $g_i(x_1, \ldots, x_n)$, $i = 1, \ldots, m$, are operations belonging to $\mathbf{A}^{(n)}$, then the operation

$$f(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$$

belongs to $\mathbf{A}^{(n)}$.

We call $\mathbf{A} = \bigcup_{n=1}^{\infty} \mathbf{A}^{(n)}$ the class of algebraic operations of the algebra (A, F) (cf. [2]).

We shall identify a group G with the algebra (A, F) where A is the set of elements of G and F is the class composed of the unary operation x^{-1} and the binary operation xy, i. e. $F = \{x^{-1}, xy\}$. Then it is easily seen that $\mathbf{A}$ is the class of all operations $f(x_1, \ldots, x_n)$ which are given by words in G, i. e. which are of the form

$$f(x_1, \ldots, x_n) = x_{i_1}^{m_1} x_{i_2}^{m_2} \ldots x_{i_l}^{m_l} \tag{1}$$

where $m_1, \ldots, m_l$ are arbitrary integers, $i_1, \ldots, i_l \in \{1, \ldots, n\}$, and $n = 1, 2, \ldots$.

Definition. Let $\mathfrak{A}_1 = (A_1, F_1)$ and $\mathfrak{A}_2 = (A_2, F_2)$ be two algebras and let $\mathbf{A}_1, \mathbf{A}_2$ be the corresponding classes of algebraic operations. We say, following E. MARCZEWSKI, that a one-to-one mapping τ of the set $A_1 \cup \mathbf{A}_1$ onto the set $A_2 \cup \mathbf{A}_2$ is a *weak isomorphism* of $\mathfrak{A}_1$ onto $\mathfrak{A}_2$ if

(k) $\qquad A_1\tau = A_2, \ \mathbf{A}_1^{(n)}\tau = \mathbf{A}_2^{(n)}$ for every n,

(kk) $\qquad$ if $f \in \mathbf{A}_1^{(n)}$, then $[f(a_1, \ldots, a_n)]\tau = (f\tau)(a_1\tau, \ldots, a_n\tau)$ for every $a_1, \ldots, a_n$ *in* A_1.

If the algebras $\mathfrak{A}_1$ and $\mathfrak{A}_2$ coincide, then we call τ a *weak automorphism* of $\mathfrak{A}[=\mathfrak{A}_1 = \mathfrak{A}_2]$.

A weak isomorphism τ of the algebras $\mathfrak{A}_1$ and $\mathfrak{A}_2$ is an isomorphism in the usual sense if $F_1\tau = F_2$. A weak automorphism of $\mathfrak{A}$ is an automorphism in the usual sense if it is the identity mapping on F.

EXAMPLE. Let $G = (A, \{x^{-1}, xy\})$ be a group. We define a weak automorphism τ of G by

(k_1) $\qquad x\tau = x^{-1}$ for every in A,

(k_2) $\qquad$ if $f \in A^{(n)}$ is of the form (1),

$$(f\tau)(x_1, \ldots, x_n) = x_{i_l}^{m_l} x_{i_{l-1}}^{m_{l-1}} \ldots x_{i_1}^{m_1}.$$

We call this weak automorphism *natural*.

PROBLEM (E. MARCZEWSKI): Do there exist two groups G and H such that there is a weak isomorphism of G onto H which is neither an isomorphism (in the usual sense) nor a combination of an isomorphism with the natural weak automorphism of one of the groups?

We give in the sequel a positive answer to this question. In fact, we prove that there is a finite group G which admits a weak automorphism τ such that τ is neither an automorphism nor a combination of an automorphism with the natural weak automorphism.

2. Results. In the sequel we deal only with nilpotent groups of class 2. It is well known that if G is nilpotent of class 2, then every word

$$x^{k_1}y^{l_1}x^{k_2}\dots x^{k_r}y^{l_r} \qquad (k_i, l_i \text{ integers})$$

is identically equal to a word of the form $x^a y^b [x, y]^k$ where the integers a, b and k depend only on $k_1, l_1, \dots, k_r, l_r$. Thus in particular the operation $x \circ y$ considered in Property ($\ast$) must be of the form $x^a y^b [x, y]^k$. We shall prove the following two theorems.

Theorem 1. *If G is a nilpotent group of class* **2**, *then a binary operation $x \circ y$ in G has properties* (i) *and* (ii) *(cf.($\ast$)) if and only if*

$$x \circ y = xy[x, y]^k \tag{2}$$

where k is any integer such that $2k+1$ is prime to the exponent n of the derived subgroup G' of G.

Then, if and only if m is an integer such that $k+m(2k+1)$ is divisible by n), we have that*

$$xy = x \circ y \circ [x, y]_\circ^m \tag{3}$$

where $[x, y]_\circ^m$ is the m-th power of the commutator of the elements x, y with respect to the multiplication $\circ$ in $G_\circ$.

REMARK. This theorem answers the problem of HIGMAN and NEUMANN (quoted above) in the affirmative. Another consequence of Theorem 1 is that a free nilpotent group of class 2 does not possess Property ($\ast$). For if Γ is free nilpotent of class 2 and an operation $x \circ y = xy[x, y]^k$ in Γ has properties (i) and (ii), then clearly this operation will have these properties in any homomorphic image G of Γ. But in the *solution of* MARCZEWSKI's *problem* below we define, for every $n > 1$, a group G with two generators which is nilpotent of class 2 and such that the exponent of its derived subgroup is n. We conclude, by Theorem 1, that $2k+1$ is prime to every $n > 1$, i. e. $k = 0$ or -1. Therefore $x \circ y = xy$ or yx, and these are the only two operations in Γ which have the properties (i) and (ii).

Theorem 2. *If G is a periodic nilpotent group of class 2 which has Property ($\ast$), then the groups G and $G_\circ$ are isomorphic.*

Postponing the proofs of these theorems to the next section we give now the *solution of* MARCZEWSKI's *problem.*

*) The existence of such an integer m follows from the fact that $2k+1$ is prime to n.

We observe first that, for every integer $n > 1$, there is a finite group G which is nilpotent of class 2 and such that the exponent of the derived subgroup G' is n. In fact, let C be the cyclic group of order n and let the group G be defined as the splitting extension of the direct product $C \times C = \{(a, b) | a, b \in C\}$ by the automorphism α

$$(a, b)^\alpha = (a, ab) \quad \text{for all} \quad a, b \quad \text{in} \quad C.$$

Then it is easily checked that $G' = \{(1, a) | a \in C\}$. Hence G' is in the centre of G, and G' has exponent n. (For our previous application note that the two elements α, $(a, 1)$ generate G whenever a is a generator of C).

Now let k be any integer such that $k \not\equiv 0, -1 \pmod n$ and $(2k+1, n) = 1$ (e. g. $k = 1$ if $n = 4$). Then the operation $x \circ y = xy[x, y]^k$ is different from the operations xy and yx, and, by Theorem 1, $x \circ y$ has the properties (i) and (ii). Hence G has Property ($*$). By Theorem 2, there is an isomorphism φ of G onto $G_\circ$, i. e. a mapping φ such that

(4) $$(xy)\varphi = x\varphi \circ y\varphi \quad \text{for all} \quad x, y \quad \text{in} \quad G.$$

To define a weak automorphism of G, we consider G as the algebra $(A, \{x^{-1}, xy\})$ where A is the set of elements of G. Denoting by $\mathbf{A}^{(n)}$ the class of algebraic operations of n variables and by $\mathbf{A}$ the class of algebraic operations, we define the mapping τ of $A \cup \mathbf{A}$ onto itself as follows

(k_1') $$x\tau = x\varphi \quad \text{for all} \quad x \quad \text{in} \quad A,$$

(k_2') if $f \in \mathbf{A}^{(n)}$ is of the form (1), then

$$(f\tau)(x_1, \dots, x_n) = [x_{i_1}]_\circ^{m_1} \circ [x_{i_2}]_\circ^{m_2} \circ \dots \circ [x_{i_l}]_\circ^{m_l}$$

where, as in (ii), $[x]_\circ^m$ denotes the m-th power of x in $G_\circ$. Then τ is a weak automorphism of G. The mapping τ is well defined, for if $f, g \in \mathbf{A}^{(n)}$ are such that $f = g$ holds identically in G, then $f\tau = g\tau$ holds identically in $G_\circ$, because G and $G_\circ$ are isomorphic. Hence $f = g$ implies $f\tau = g\tau$. By the same argument, $f\tau = g\tau$ implies $f = g$, and thus τ is one-to-one on $\mathbf{A}$. We also have that τ is one-to-one on A, because τ is an isomorphism of G onto $G_\circ$. From (3) it follows that τ maps $\mathbf{A}$ onto $\mathbf{A}$ and thus, by (4), τ is a weak automorphism. But τ is not an automorphism nor a combination of an automorphism with the natural weak automorphism, because the τ-image of the operation xy, i. e. the operation $x \circ y = xy[x, y]^k$, is different from both xy and yx.

3. Proofs of the Theorems. Before proving the theorems we wish to recall some well known identities valid in any nilpotent group of class 2. If G is a nilpotent group of class 2, then for any x, y, z in G and any integer n the following identities hold:

(5) $$(xy)^n = x^n y^n [y, x]^{\frac{n(n-1)}{2}}$$

(6) $$[xy, z] = [x, z][y, z], \ [x, yz] = [x, y][x, z],$$

hence

(7) $$[x^n, y] = [x, y^n] = [x, y]^n.$$

PROOF OF THEOREM 1. Let G be a nilpotent group of class 2 and let $x \circ y$ be an operation in G which has the properties (i) and (ii) (cf. $(*)$). Then, as we observed at the beginning of the previous section

$$x \circ y = x^a y^b [x, y]^k$$

for all x, y in G and some integers a, b, k. Let 1 be the unit element of G. By the above equality, $1 \circ 1 = 1$, hence 1 is also the unit element of $G_\circ$. Therefore

$$x = x \circ 1 = x^a, \ y = 1 \circ y = y^b$$

hold identically in G, and we have (2). It follows immediately from (2) that, for every integer n, the n-th power of any element x with respect to the operation $\circ$ is just x^n. Also, the commutator $[x, y]_\circ$ in $G_\circ$ can be easily expressed in terms of the commutator $[x, y]$. In fact, a simple application of (2), (6), and (7) shows that

$$[x, y]_\circ = [x, y]^{2k+1}. \tag{8}$$

Hence $\big[[x, y]_\circ, z\big]_\circ = \big[[x, y]^{2k+1}, z\big]^{2k+1} = 1$, i. e. $G_\circ$ is nilpotent of class 2. From this and from (ii) we infer that for some integers a, b, m

$$xy = x^a \circ y^b \circ [x, y]_\circ^m.$$

The argument used to prove (2) will also serve now to prove that (3) holds identically for all x, y in G.

We note that, by (8), $[x, y]_\circ^m = [x, y]^{m(2k+1)}$. Substituting this in (3) and using (2) we get

$$xy = xy[x, y]^{k+m(2k+1)}$$

valid for all x, y in G. Hence the order of each commutator $[x, y]$ must divide $k + m(2k+1)$ and so, as G is nilpotent of class 2, the exponent n of the derived subgroup G' of G must also divide $k + m(2k+1)$. It follows that $2k+1$ is prime to n. This completes the proof of the necessity of the conditions.

To prove the sufficiency, we suppose that G is a nilpotent group of class 2 and that k is an integer such that $2k+1$ is prime to the exponent n of the derived subgroup G'. In this case there is an integer m such that $k + m(2k+1)$ is divisible by n.

To prove (i), we observe first that the operation (2) is associative. In fact, by (7),

$$(x \circ y) \circ z = xyz[x, y]^k [x, z]^k [y, z]^k = x \circ (y \circ z).$$

We also have $1 \circ x = x \circ 1 = x$ and $x^{-1} \circ x = x \circ x^{-1} = 1$, so that the elements of G form a group $G_\circ$ under the multiplication $x \circ y$.

To prove (ii) we note that, as before, we have (8); whence, applying (2), we deduce that

$$x \circ y \circ [x, y]_\circ^m = xy[x, y]^{k+m(2k+1)}.$$

Using the fact that the exponent of G' divides $k + m(2k+1)$, we obtain (3). This completes the proof of the theorem.

PROOF OF THEOREM 2. The following well known lemma will be applied in the proof.

Lemma. *If G is a periodic nilpotent group, then G is the direct product of its Sylow p-groups.*

We now assume that G is a periodic nilpotent group of class 2 which has Property $(*)$. Then, by Theorem 1, the operation $x \circ y$ is of the form (2) and there is an integer m such that (3) holds. Moreover, the exponent of the derived subgroup G' of G divides the number $t = k + m(2k+1)$.

Let $t = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ be the factorization of t into primes and let

$$P = P_1 \times \dots \times P_r$$

be the direct product of the Sylow p_i-subgroups $(i = 1, \dots, r)$ of the group G. Then, by the lemma,

$$G = P \times Q.$$

Of course each element of Q has order prime to t. Moreover, the group Q is Abelian. For if x, y are in Q, then, since the exponent of G' divides t, $[x, y]$ must belong to P, so $[x, y] \in P \cap Q = \{1\}$. We note that also

$$G_\circ = P_\circ \times Q_\circ,$$

where $P_\circ$ and $Q_\circ$ are the groups formed from the elements of P and Q respectively under the multiplication $x \circ y$.

Let $s = 2m+1$. We have that s is prime to t, for $(2m+1, m+(2m+1)k) = d$ implies $d \mid 2m+1$, whence $d \mid m$, and so $d \mid 1$. We define now a mapping φ of G onto $G_\circ$ by

$$a\varphi = a^s \quad \text{if} \quad a \quad \text{is in} \quad P,$$

$$b\varphi = b \quad \text{if} \quad b \quad \text{is in} \quad Q,$$

$$(ab)\varphi = a\varphi \circ b\varphi \quad \text{for any} \quad a \quad \text{in} \quad P \quad \text{and} \quad b \quad \text{in} \quad Q.$$

It is clear that, by $(s, t) = 1$, s is prime to the orders of the elements of P, hence φ is one-to-one and onto. We prove that φ is an isomorphism of G onto $G_\circ$. To this purpose it is sufficient to prove that φ is a homomorphism on P. If x, y are in P, we have, by (5),

$$(xy)\varphi = (xy)^s = x^s y^s [y, x]^{\frac{s(s-1)}{2}} = x^s y^s [x, y]^{\frac{s(1-s)}{2}}.$$

On the other hand, by (2) and (7),

$$x\varphi \circ y\varphi = x^s \circ y^s = x^s y^s [x^s, y^s]^k = x^s y^s [x, y]^{s^2 k}.$$

Thus all that remains to prove is that

$$\frac{s(1-s)}{2} \equiv s^2 k \pmod{n}$$

where n is the exponent of G'. But this is immediate, for we have $n \mid t$ and

$$s^2 k - \frac{s(1-s)}{2} = s\left(sk - \frac{1-s}{2}\right) = s\big((2m+1)k + m\big) = st.$$

Bibliography

[1] G. HIGMAN and B. H. NEUMANN, Groups as groupoids with one law, *Publ. Math. Debrecen* **2** (1952), 215—221.
[2] E. MARCZEWSKI, A general scheme of notions of independence in mathematics, *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astr. Phys.* **6** (1958), 731—736.
[3] HANNA NEUMANN, On a question of Kertész, *Publ. Math. Debrecen* **8** (1961), 75—78.

(Received January 23, 1962.)