Consequently, it suffices to prove then

$$A^i B^j \Phi(A,B) = A^i B^j \Phi(X^i, X^j)$$

or, in other terms,

$$A^i B^j \Phi(A,B) \dot{-} A^i B^j \Phi(X^i, X^j) = 0. \tag{13}$$

By the quasi-analyticity of Φ and the relations (9) and (10) we have

$$A^i B^j \Phi(A,B) \dot{-} A^i B^j \Phi(X^i X^j) =$$
$$= A^i B^j [\Phi(X^i, X^j) \dot{-} \Phi(A,B)] \subset A^i B^j [(X^i \dot{-} A) + (X^j \dot{-} B)] =$$
$$= A^i B^j A^{1-i} + A^i B^j B^{1-j} = 0,$$

whence the equality (13).

By Lemma 1 we obtain immediately the

Lemma 2. *If for a quasi-analytical operation $\Phi(A,B)$ holds*

$$\Phi(0,0) = \Phi(X,X) = 0 \quad \textit{and} \quad \Phi(0,X) = \Phi(X,0) = X,$$

then we have identically $\Phi(A,B) = A \dot{-} B$.

Theorem. *Suppose a binary quasi-analytical operation $\circ$ is defined in a family $\boldsymbol{F}$ of elements of a Boolean algebra $\boldsymbol{B}$ such that the „empty" element 0 and the „universal" element X of $\boldsymbol{B}$ belong to $\boldsymbol{F}$ and that $\boldsymbol{F}$ is a group with respect to $\circ$, with „empty" element as unit. Then*

$$A \circ B = A \dot{-} B \quad \textit{for each} \quad A, B \in \boldsymbol{F}. \tag{14}$$

Proof. By group properties,

$$0 \circ 0 = 0, \quad 0 \circ X = X \quad \text{and} \quad X \circ 0 = X \tag{15}$$

By formula (12) of Lemma 1 and by (15) we have

$$A \circ X \supset (X - A) X (0 \circ X) = X - A \quad \text{for} \quad A \in \boldsymbol{F},$$

whence $A \circ X \neq 0$ for $A \neq X$. On the other hand, there is by group properties a $B \in \boldsymbol{F}$ such that $B \circ X = 0$, whence

$$X \circ X = 0. \tag{16}$$

By (15), (16) and Lemma 2 we obtain (14), q. e. d.

ON THE SYMMETRIC DIFFERENCE OF SETS AS A GROUP OPERATION

BY

HENRY HELSON (CAMBRIDGE, MASS.)

If M is a set of elements $a, b, \ldots$ and $\boldsymbol{M}$ the field of all subsets $A, B, \ldots$ of M, then $\boldsymbol{M}$ is a group under the point-set operation symmetric difference:

$$A \dot{-} B = (A - B) + (B - A).$$

Evidently the group is completely determined by the power of M, and is commutative [1]).

Suppose $\boldsymbol{M}$ is a group with respect to some binary operation $\circ$. S. Ulam has asked what further conditions can be imposed on $\circ$ to characterize the operation as symmetric difference. Marczewski has shown [2]) that quasi-analyticity is a sufficient condition. The purpose of this note [3]) is to give another such condition, related to the definition of binary G-operations of Marczewski [4]).

Le φ be a one-one transformation of $\boldsymbol{M}$ into itself. Define φ to be *simple* if $\varphi(a) = b$, $\varphi(b) = a$ for some pair of points $a, b \in M$, and $\varphi(c) = c$ for all other points $c \in M$; that is, φ simply inter-

---

[1]) It follows by the known theorems on groups every element of which has order at most 2 (cf e. g. L. Pontriagin, *Topological Groups*, Princeton 1940, p. 19, Example 9) that every group of this type is isomorphic to the group of all finite subsets of a set (with symmetric difference as the group operation).

[2]) This fascicle, pp. 199-202.

[3]) Written at the University of Wrocław while the author held a Sheldon Travelling Fellowship from Harvard University.

[4]) E. Szpilrajn-Marczewski, Annales de la Société Polonaise de Mathématique 17, 1938, p. 123-124. A binary G-operation is invariant under all one-one mappings of M into itself, and so is invariant under simple transformations. For an example of an operation defined in the space of integers invariant under simple transformations which is not a G-operation, define sets A and B to be equivalent just if one can be obtained from the other by a finite number of simple transformations, and set $A \circ B = 0$ or M according as A and B are not, or are, equivalent.

changes a pair of points. Evidently, symmetric difference is invariant under simple transformations; that is, $\varphi(A \dot{-} B) = \varphi(A) \dot{-} \varphi(B)$. Assume now that $\circ$ is a group operation defined in $\boldsymbol{M}$ with the empty set as zero, invariant under simple transformations. Let A^* denote the inverse of A.

We first prove three lemmas.

Lemma 1. Either $A \cdot A^* = 0$ or $A \cdot A^* = A$.

For assume both false. Then there is some $a \epsilon A - A^*$, and $b \epsilon A \cdot A^*$. The transformation carrying a into b and leaving other points fixed is simple; but $\varphi(A \circ A^*) = \varphi(0) = 0$, while $\varphi(A) \circ \varphi(A^*) \neq 0$ because $\varphi(A) = A$, $\varphi(A^*) \neq A^*$. This contradicts the assumption that $\circ$ is invariant under simple transformations.

Lemma 2. Either $A^* = A$ or $A^* = A'$ (where A' denote the complement of A).

If $A \cdot A^* \neq 0$, by lemma 1 we have symmetrically

$$A \cdot A^* = A \qquad \text{and} \qquad A^* \cdot A = A^*.$$

Hence $A = A^*$.

If $A \cdot A^* = 0$, and $a \epsilon M - (A + A^*)$, we can choose any $b \epsilon A^*$ (since we can suppose $A^* \neq 0$) and define a simple transformation φ carrying a into b and leaving other points fixed. Then φ transforms A^* into a different set, but leaves A and $A \circ A^* = 0$ fixed, a contradiction as before. Hence $M - (A + A^*) = 0$ and $A^* = A'$.

Lemma 3. For every A, $A \circ A = 0$ or $A \circ A = M$.

If $A^* = A$, then $A \circ A = 0$. Otherwise, by lemma 1, $A \circ A' = 0$. It follows that A is not 0 or M, and so if $A \circ X = M$, X is not 0 or M. Arguments like those used above show that X then has to be A or A', but since A' is the inverse of A, the lemma is shown.

By lemma 3, since $M \circ M = 0$, every element of $\boldsymbol{M}$ has order 2 or 4.

The following example shows that there may actually be elements of order 4 present. Take M the set of two elements a and b, with subsets $\{0\}, \{a\}, \{b\}$, and $\{a, b\}$ which we write simply $0, a, b$ and ab. Define $\circ$ by the following table:

$\circ$	0	a	b	ab
0	0	a	b	ab
a	a	ab	0	b
b	b	0	ab	a
ab	ab	b	a	0

Then $\circ$ is invariant under permutation of a and b, and a and b have order 4. However, assume now, not only that $\circ$ is invariant under simple transformations, but that the following condition holds: for all A and B, $A \circ B \subset A + B$. Under these hypotheses we can prove the uniqueness of $\circ$.

Lemma 4. If $A \cdot B = 0$, $A \circ B = A + B$.

Unless $A = B = 0$, $A \circ B \neq 0$. The operation $\circ$ being invariant under simple transformations, if $A \circ B$ intersects A, evidently $A \subset A \circ B$, and similarly for B. By the new hypothesis on $\circ$ it follows that $A \circ B$ can only be A, B or $A + B$. But the first two possibilities are excluded by group properties unless A or B is 0.

Theorem. If $\circ$ is a group operator on the subsets of a set M with zero the empty set, invariant under simple transformations, such that $A \circ B \subset A + B$ for all subsets A, B of M, then $\circ$ is symmetric difference.

By lemma 3, every element is its own inverse. This fact and lemma 4 establish the following equalities:

$$A \circ B = [(A - B) + (A \cdot B)] \circ B = [(A - B) \circ (A \cdot B)] \circ B =$$
$$= (A - B) \circ (A \cdot B) \circ (A \cdot B) \circ (B - A) = (A - B) + (B - A).$$

Wrocław, May 1948.