[10] — *Crumpled cubes*, Topology Seminar, Wisconsin 1965, Ann. Math. Studies 60, Princeton, N. J.

[11] F. M. Lister, *Simplifying intersection of disks in Bing's Side Approximation Theorem*, Pac. J. Math. 22 (1967), pp. 281-295.

[12] J. Martin, *The sum of two crumpled cubes*, Mich. Math. J. 13 (1966), pp. 147-151.

[13] — *A rigid sphere*, Fund. Math. 59 (1966), pp. 117-121.

Reçu par la Rédaction le 16. 1. 1968

A note on inverse binary operation in abelian groups

by

R. Padmanabhan (Winnipeg)

It is well known that in a group $\langle G, +, -, 0\rangle$, all the group operations can be expressed in terms of a single binary operation $a*b = a-b$. Thus, $0 = a*a$, $-a = 0*a$ and $a+b = a*(-b)$. It is not known whether the 'right subtraction', the 'left subtraction' and its transposes are the only binary operations in groups in terms of which all the other group operations can be expressed. However, in [1], Higman and Neumann have stated that, in the case of abelian groups, these are the only operations having the property and Professor Neumann says (1) that there exists no explicit publication of the proof so far. In this note we give a proof for the same.

Notations and definitions. A binary operation in a group $\langle G, +, -, 0\rangle$ is a *word in two symbols*, say a, b and in the group symbols $+$ and $-$. It is known that any word in a, b in an abelian group can be written in the form $ma+nb$ where m and n are integers (ma stands for '$a+a+\ldots$ m times'). If $f(a, b)$ is the word $ma+nb$, then the *length* of the word f is, as usual, the positive integer $|m|+|n|$, while the 'degree' of the word f is, by definition, the integer $m+n$.

THEOREM. *If $a*b$ is a binary operation in an abelian group $\langle G, +, -, 0\rangle$, in terms of which all the other group operations can be expressed, then $a*b = a-b$ or else $a*b = b-a$.*

Proof. Given that

$$a+b = g(a, b)\,, \quad \text{some word in the binary system } \langle G, *\rangle\,,$$

$$-a = h(a)\,, \quad \text{some word in the binary system } \langle G, *\rangle\,,$$

and so, (or even otherwise)

$$\begin{aligned} 0 &= a+(-a) \\ &= g\big(a, h(a)\big) \\ &= f(a)\,, \quad \text{some word in } \langle G, *\rangle\,. \end{aligned}$$

Moreover, we have $G+G = G$, i.e. given a in G, there exist elements b, c in G such that $a = b+c$, or $a = g(b, c) = u*v$, where u and v are words in b, c and the symbol $*$. So we have $G*G = G$.

(1) In a private communication.

Since G is an abelian group, we have $a*b = ma+nb$, where m and n are integers. First of all, it is easy to observe that neither m nor n can be zero. For, if $m = 0$, then $a*b = nb$, and hence, in the additive group of integers Z, for example, $Z*Z \neq Z$. (2)

If m and n are both positive integers then

$$a*a = (m+n)a \quad \text{and} \quad a*(a*a) = (2m+n)a\,, \quad \text{and so on,}$$

i.e. if the length of the polynomial on a increases, then its degree will also increase. Thus in Z, for example, no word $f(a)$ will be identically zero. Similarly m and n cannot both be negative. Thus m and n are of opposite sign.

Let $a*b = ma-nb$, where m and n are now positive integers.

Let us assume that $m > n$.

Case i: $n \neq 1$. Let $m = n+k$ (since $m > n$)

$$\begin{aligned} a*b &= (n+k)a-nb \\ &= n(a-b)+ka\,. \end{aligned}$$

Consider Z_n — the additive group of integers (mod n). Here $a*b = ka$. We have

$$\begin{aligned} a+b &= g(a,b) \\ &= g_1(a,b)*h_1(a,b) \\ &= kg_1(a,b) \\ &= k\big(g_2(a,b)*h_2(a,b)\big) \\ &= k^2g_2(a,b) \\ &= \ldots \\ &= k^pg_p(a,b) \end{aligned}$$

where $g_p(a,b)$ is a word of length 1, i.e. $g_p(a,b) = a$ or b. Thus $a+b = k^pa$ or $a+b = k^pb$. In the first case we get, e.g., that $b = 0+b = k^p0 = 0$ while in the second case, by a similar argument, we get $a = 0$ which is a contradiction since in Z_n ($n \neq 1$) there are at least two elements. Thus the case $n \neq 1$ is impossible.

Case ii: $n = 1$ (therefore $m \neq 1$).

$$\begin{aligned} a*b &= ma-b\,, \\ a*a &= ma-a = (m-1)a\,. \end{aligned}$$

Let $f(a)$ be of degree p and $g(a)$ of degree q. Then $f(a)*g(a) = (pa)*(qa) = (mp-q)a$ has degree $mp-q$. Thus if $h(a) = f(a)*g(a) = 0$, then $mp-q = 0$, i.e. $mp = q$. Hence we conclude that if for some word $h(a)$, $h(a)$ is identically zero, then it implies that there exists a polynomial (in a) whose degree is a multiple of m.

(2) This argument fails if $n=1$. However, if $n=1$ then no word $f(a)$ will be identically zero. I am thankful to referee for this remark.

LEMMA. *In the groupoid* $\langle G, * \rangle$ *where* $a*b = ma-b$, *there exists no polynomial* (*on a single letter, say* a) *whose degree is a multiple of* m.

The proof is by induction on the length of the word $f(a)$. If $f(a)$ is of length 2 (i.e. $f(a) = a*a$), then its degree is $m-1$ and hence it is not a multiple of m (since $m \neq 1$).

Let the statement of the lemma be true for all words $f(a)$ of length less than or equal to k.

Let $f(a)$ be a word of length $k+1$, so $f(a) = x(a)*y(a)$ where x and y are words of length less than or equal to k and hence their degrees d_x and d_y are not multiples of m. Therefore degree $f(a) = md_x-d_y$ is not a multiple of m. The proof of the lemma is complete.

Thus, the integer m cannot be greater than n. Similarly one can show that m cannot be less than n. Therefore $m = n$. Consider the abelian group Z again. We have $a*b = m(a-b)$ and unless we have $m = 1$ we have $Z*Z \neq Z$. Thus $a*b = a-b$.

Similarly in the other case where $a*b = -ma+nb$ where m and n are $+ve$ we get $a*b = -a+b$. This completes the proof of the theorem.

Added in proof (29. 3. 68): A. Hulanicki and S. Świerczkowski in their paper *On group operations other than xy or yx*, Publ. Math. Debrecen 9 (1962) 142-148, have claimed to have given an affirmative solution to the problem of Higman and Neumann mentioned in the first paragraph of this paper. What actually they have shown is the existence of a group G in which there exists a binary word other than $a-b$ or $b-a$ in terms of which all the other operations of G can be expressed. But the question here is not whether there exists a group G with the stated properties but whether there exists a binary group word which works universally for all groups. In fact, the question interpreted in the former way can be easily answered even in the case of abelian groups: Considering the word $a*b = 3a+2b$ in Z_5 the additive group of integers (mod 5), we have $(a*b)*(b*b) = -a+b$ and hence all the words of Z_5 can be expressed in terms of $*$, but e. g., $2-3 \neq 2*3 = 2 \neq 3-2$. But Higman and Neuman have themselves observed (last sentence, page 221 of [1]) that in abelian groups the left division and the right division are the only operations with the desired properties. The general problem appears to be open.

References

[1] G. Higman and B. H. Neumann, *Groups as groupoids with one law*, Publ. Math. Debrecen 2 (1952), pp. 215-221.

MADURAI UNIVERSITY
Madurai, India
UNIVERSITY OF MANITOBA
Winnipeg, Canada

Reçu par la Rédaction le 30. 1. 1968