ON PRODUCTS OF SETS OF GROUP ELEMENTS

HENRY B. MANN

LET $\mathfrak{A} = \{A_1, \ldots, A_s\}$, $\mathfrak{B} = \{B_1, \ldots, B_t\}$ be sets of elements of a group $\mathfrak{G}$ of finite order g. We define

$$\mathfrak{C} = \mathfrak{A}\mathfrak{B} = \{A_i B_j\}.$$

By $(\mathfrak{A})$, $(\mathfrak{B})$, ... we shall denote the number of elements in $\mathfrak{A}$, $\mathfrak{B}$, ... respectively and by $\overline{\mathfrak{A}}$, $\overline{\mathfrak{B}}$, ... the sets of elements of $\mathfrak{G}$ not in $\mathfrak{A}$,$\mathfrak{B}$, ...

THEOREM 1. *Either* $\mathfrak{A}\mathfrak{B} = \mathfrak{G}$ *or* $g \geqslant (\mathfrak{A}) + (\mathfrak{B})$.

Proof. Let $\overline{C}$ be an element not in $\mathfrak{C} = \mathfrak{A}\mathfrak{B}$. Let $A, B, \ldots$ be a generic notation for elements in $\mathfrak{A}$, $\mathfrak{B}$, ... respectively. All A are different from all $\overline{C}B^{-1}$ for otherwise $\overline{C} = AB$. Thus there are at least $(\mathfrak{A}) + (\mathfrak{B})$ elements in $\mathfrak{G}$.

THEOREM 2. *Let* $\mathfrak{A}$, $\mathfrak{B}$ *be sets of elements of an Abelian group* $\mathfrak{G}$ *and let* $\overline{C} \subset \overline{\mathfrak{A}\mathfrak{B}}$. *Then there exists a* $\mathfrak{B}^* \supseteq \mathfrak{B}$ *such that*

(i) $\overline{\mathfrak{C}}^* = \overline{\mathfrak{A}\mathfrak{B}^*} = \mathfrak{H}\overline{C}$, *where* $\mathfrak{H}$ *is a subgroup of* $\mathfrak{G}$,

(ii) $(\mathfrak{A}\mathfrak{B}^*) - (\mathfrak{A}\mathfrak{B}) = (\mathfrak{B}^*) - (\mathfrak{B})$.

We shall give the proof by induction on the number of elements in $\overline{\mathfrak{C}}$. Clearly Theorem 2 holds with $\mathfrak{H} = I$ the identity if $\overline{\mathfrak{C}}$ consists only of one element $\overline{C}$. Now let $\overline{\mathfrak{C}}$ consist of the elements $\overline{C} = \overline{C}_0, \overline{C}_1, \ldots, \overline{C}_s$. Form the products $\overline{C}\,\overline{C}_i^{-1} = D_i$ and let $\mathfrak{H}$ be the subgroup generated by the D_i. Two cases arise.

First case. For every i and k we have for some m

$$\overline{C}_i D_k^{-1} = \overline{C}_m.$$

Since $\overline{C}_i = \overline{C}D_i^{-1}$ it then follows that for every $H \subset \mathfrak{H}$ we have for some m

$$\overline{C}H = \overline{C}_m.$$

Since $\overline{C}D_m^{-1} = \overline{C}_m$, so that $\overline{C}_m = \overline{C}H$ for every m, it follows that $\overline{\mathfrak{C}} = \overline{C}\mathfrak{H}$.

Second case. There exist an i and a k such that

$$\overline{C}_i D_k^{-1} = AE, \quad E \subset \mathfrak{B}.$$

We then form the set $\mathfrak{B}_1$ consisting of all elements of the form ED_j which satisfy an equation

(1) $$AED_j = \overline{C}_t$$

Received August 2, 1950.

for some t. Equation (1) implies also

$$AED_t = \bar{C}_j. \tag{1'}$$

We shall prove:

PROPOSITION 1. *No element of* $\mathfrak{B}_1$ *is in* $\mathfrak{B}$. This follows easily since no element in $\mathfrak{B}$ can satisfy an equation of the form (1).

PROPOSITION 2. *Let* $\mathfrak{B} \cup \mathfrak{B}_1 = \mathfrak{B}_1{}^*$ *then* $\mathfrak{C}_1 = \mathfrak{A}\mathfrak{B}_1{}^* \not\supset \bar{C}$. Otherwise we should have $AED_j = \bar{C}$, $AE = \bar{C}_j$ which is impossible since $E \subset \mathfrak{B}$ but $\bar{C}_j \not\subset \mathfrak{A}\mathfrak{B}$.

PROPOSITION 3. $(\mathfrak{A}\mathfrak{B}_1{}^*) - (\mathfrak{A}\mathfrak{B}) = (\mathfrak{B}_1{}^*) - (\mathfrak{B}) = (\mathfrak{B}_1)$.

Equations (1) and (1′) show that ED_j is in $\mathfrak{B}_1$ if and only if $\bar{C}_j \subset \mathfrak{C}_1 = \mathfrak{A}\mathfrak{B}_1{}^*$ which proves Proposition 3.

Since $(\bar{\mathfrak{C}}_1) < (\bar{\mathfrak{C}})$ there exists by induction a set $\mathfrak{B}^* \supset \mathfrak{B}_1{}^* \supset \mathfrak{B}$ such that $\overline{\mathfrak{A}\mathfrak{B}^*} = \bar{C}\mathfrak{H}$ where $\mathfrak{H}$ is a subgroup of $\mathfrak{G}$ and such that

$$(\mathfrak{A}\mathfrak{B}^*) - (\mathfrak{A}\mathfrak{B}_1{}^*) = (\mathfrak{B}^*) - (\mathfrak{B}_1{}^*).$$

Adding this equation to Proposition 3 we obtain Theorem 2.

COROLLARY (Davenport and Chowla). *Let* $\mathfrak{G}$ *be the additive group of residues* mod N. *Let* $\mathfrak{A} = \{a_0 = 0, a_1, \ldots, a_m\}$, $\mathfrak{B} = \{b_1, \ldots, b_m\}$ *be sets of residues* mod N *such that* $(a_i, N) = 1$ *for* $i > 0$. *Let* $\mathfrak{C} = \mathfrak{A}\mathfrak{B}$. *Then either* $\mathfrak{C} = \mathfrak{G}$ *or*

$$(\mathfrak{C}) \geqslant m + n = (\mathfrak{A}) + (\mathfrak{B}) - 1. \tag{2}$$

Proof. By Theorems 1 and 2 it is sufficient to prove the Corollary for the case that $\bar{\mathfrak{C}} = \bar{C}\mathfrak{H}$ where $\mathfrak{H}$ is a subgroup of $\mathfrak{G}$. Consider the factor group $\mathfrak{G}/\mathfrak{H}$. Let $\mathfrak{A}'$, $\mathfrak{B}'$ be the sets of cosets mod $\mathfrak{H}$ that contain elements of $\mathfrak{A}$ and $\mathfrak{B}$ respectively. Let t be the index and h the order of $\mathfrak{H}$. By Theorem 1,

$$t \geqslant (\mathfrak{A}') + (\mathfrak{B}').$$

Hence

$$N = ht \geqslant h(\mathfrak{A}') + h(\mathfrak{B}'). \tag{3}$$

Since $a_0 \subset \mathfrak{H}$, $a_i \not\subset \mathfrak{H}$ for $i > 0$, we have

$$h(\mathfrak{A}') - h \geqslant m, \; h(\mathfrak{B}') \geqslant n.$$

Substituting this in (3) we obtain

$$N \geqslant m + n + h, \quad (\mathfrak{C}) = N - h \geqslant m + n.$$

The Corollary to Theorem 2 was proved by Davenport [**2**] for the case that N is a prime. Chowla [**1**] used Davenport's methods to obtain the Corollary in its general form. Davenport later discovered that for the case when N is a prime the Corollary was already known to Cauchy [**3**].

It is interesting to note that the proof of Theorem 2 is closely related to the author's proof of the fundamental theorem on the density of sums of sets of positive integers [**4**]. Thus the similarity between this theorem and the theorem of Davenport and Chowla is not as superficial as might have appeared.

References

1. I. Chowla, Proc. Indian Acad. Sci., vol. 2 (1935), 242-243.
2. H. Davenport, J. Lond. Math. Soc., vol. 10 (1935), 30-32.
3. ———, J. Lond. Math. Soc., vol. 22 (1947), 100-101.
4. H. B. Mann, Ann. of Math., vol. 43 (1942), 523-527.

Ohio State University