PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 44, Number 2, June 1974

# PROVING KNESER'S THEOREM FOR FINITE GROUPS BY ANOTHER $e$-TRANSFORM*

R. A. LEE

ABSTRACT. Although neither the result nor the $e$-transformation is new, a new order for the successive transformations is prescribed. From this follow some interesting properties which in turn imply the result.

Let $A$, $B$ and $C$ be subsets of a finite abelian group $G$, with $a$, $b$ and $c$ the respective elements. Suppose further that $A+B=C$.

DEFINITION. Let $\bar{A}=\{x:x+B\subset C\}$. We say $A$ is full whenever $A=\bar{A}$. Notice that $A\subset\bar{A}$ and $\bar{A}+B=C$.

DEFINITION. Let $\Delta C=\{x:x+C\subset C\}$. It is obvious that $0\in\Delta C$, $C+\Delta C\subset C$, $\Delta A\subset\Delta C$ (in fact $\Delta A=\Delta C$ if $A$ is full). Also $C+S\subset C$ implies that $S\subset\Delta C$. Hence $\Delta C+\Delta C=\Delta C$, so that $\Delta C$ is a subgroup of $G$. We now use the usual Dyson $e$-transform. H. B. Mann's $e$-transform would serve equally well with only the obvious modifications in the proof, and indeed the proof was originally done using that transform.

For $e$ in $A$, a full set, and $0\in B$ another full set,

$$\begin{aligned} A\to A' &= A\cup(B+e),\\ B\to B' &= B\cap(A-e),\\ C\to C' &= A'+B'. \end{aligned}$$

Also let

$$\begin{aligned} A^* &= \{a:a\in A',\, a\notin A\},\\ B^* &= \{b:b\in B,\, b\notin B'\}. \end{aligned}$$

We have the following usual properties:

$P_0$. $C'\subset C$,

$P_1$. $B^*+e=A^*$,

$P_2$. $|A|+|B|=|A'|+|B'|$,

$P_3$. $0\in B'$.

---

Received by the editors January 13, 1972 and, in revised form, February 15, 1973.

* This article has not been proofread by the author because the Amer. Math. Soc. was unable to locate him. The address given at the end of the paper is the last address given by the author.

For any $b'$ such that $b'+A'\subset C'$, we clearly have $b'+A\subset C$ and $b'+(B+e)\subset C$, which implies, since $A$ and $B$ are full, that $b'$ is in both $B$ and $A-e$. Thus $b'$ is in $B'$ showing that

P$_4$. $B'$ is full.

Let $H=C'$. Since $B'$ is full, $H=B'$; so that $B'+H=B'\subset A^*-e$. This implies

P$_5$. $e+B'+H\subset A$.

THEOREM. $|A|+|B|\leqq|C|+|\Delta C|$.

LEMMA 1. *For any $a$ in $A$ such that $a+B+H\not\subset C$*

$$|A\cap(a+H)|+|C'|\leqq|C|.$$

PROOF. By hypothesis, there is an element $b$ of $B$ so that $a+b+H\not\subset C$. Since $C'+H\subset C'$ and $C'\subset C$, $C'$ must be disjoint from the coset $a+b+H$. The set $[A\cap(a+H)]+b$ is contained in this coset and also in $C$. Hence $C$ has at least $|[A\cap(a+H)]+b|=|A\cap(a+H)|$ more elements than $C'$ has.

We may inductively assume the theorem to be true for any $A_1$, $B_1$ and $C_1$ such that $A_1+B_1=C_1$ and $|B_1|<|B|$. Assuming for now that $e$ can be chosen so that $|B'|<|B|$ we clearly have $(A'+H)+B'=C'$; so by the inductive assumption:

$$|A'+H|+|B'|\leqq|C'|+|H|. \tag{1}$$

LEMMA 2. *For any $a\in A$ such that $a+H\not\subset A$,*

$$|A|+|B|\leqq|C|+|A^*\cap(a+H)|.$$

PROOF. If $a+B+H$ were contained in $C$, then $a+H$ would be contained in $A$, since $A$ is full. This is, however, not the case so it follows that $a+B+H\not\subset C$. The inequality of Lemma 1 thus holds and adding this to inequality (1) and the following three easy relations yield the lemma after massive cancellation:

$$|A|+|B|=|A'|+|B'|,$$
$$|A'\cap(a+H)|=|A\cap(a+H)|+|A^*\cap(a+H)|,$$
$$|H|+|A'|\leqq|A'\cap(a+H)|+|A'+H|.$$

Let the images of $A$, $B$ and $C$ under the transformation by $d\in A$ be the sets $A'_d$, $B'_d$, $C'_d$ respectively, with difference sets $A^*_d$ and $B^*_d$.

Unless $A+B\subset A$, there must be a $d$ in $A$ with $d+B\not\subset A$. Thus $B^*_d$ is not empty. Choose $e$ in $A$ so that $B^*_e$ is not empty, but minimal in the sense that no nonempty $B^*_d$ is properly contained in it. This means that if $B^*_d\subset B^*_e$ then either $B^*_d=B^*_e$ or $B^*_d=\varnothing$. As before, we call $A'_e$, $B'_e$, $A^*_e$, and $B^*_e$ respectively $A'$, $B'$, $A^*$ and $B^*$.

By $P_3$ and $P_5$, $e+H\subset A$ so we can transform by any $e+h$, where $h\in H$. Let

$$K=\{h:h\in H,\ B^*_{e+h}=\varnothing\}.$$

LEMMA 3. *For any $a^*$ in $A^*$, $(a^*+H)\cap A=a^*+K$.*

PROOF. By $P_5$, $e+H+B'\subset A$, so that no $b'$ in $B'$ could even be removed by a transformation under $e+h$. Hence, $B^*_{e+h}\subset B^*$. Thus by the minimal choice of $e$, we have either $B^*_{e+h}=\varnothing$ or $B^*_{e+h}=B^*$. If $h$ is in $K$ then $B^*_{e+h}=\varnothing$, so that $A^*_{e+h}=\varnothing$ and $a^*+h\in B+e+h\subset A'_{e+h}=A$. If $h$ is not in $K$, $B^*_{e+h}=B^*$, so that by $P_1$, $A^*_{e+h}=e+h+B^*_{e+h}=e+h+B^*=h+A^*$. Therefore $a^*+h$ is in $A^*_{e+h}$, a set which is disjoint from $A$. This shows that $a^*+h$ is in $A$ if and only if $h$ is in $K$, proving the lemma.

LEMMA 4. *For any $a$ in $A$, $|(a+H)\cap A^*|\leqq|\Delta K|$.*

This is trivial if $(a+H)\cap A^*$ is empty, so assume it is nonempty. For any $a_1^*$ and $a_2^*$ in $(a+H)\cap A^*$, Lemma 3 implies $(a+H)\cap A=a_1^*+K=a_2^*+K$. Thus $K+(a_1^*-a_2^*)\subset K$, so that

$$((a+H)\cap A)-((a+H)\cap A^*)\subset\Delta K.$$

Moreover,

$$\begin{aligned}|(a+H)\cap A^*|&=|((a+H)\cap A^*)-a_1^*|\\&\leqq|((a+H)\cap A^*)-((a+H)\cap A^*)|\leqq|\Delta K|,\end{aligned}$$

which proves the lemma.

PROOF OF THE THEOREM. If $B$ is empty, so is $C$; making $\Delta C=G$, and the theorem trivially follows. We may thus assume $B$ is nonempty and moreover that 0 is an element of $B$ by taking translates of $B$ and $C$ if necessary. We may also assume that $A$ and $B$ are full by replacing $A$ by $\bar{A}$ and then $B$ by $\bar{B}$, since this only increases the left-hand side of the inequality.

If $B+A\subset A$, then $B\subset\Delta A=\Delta C$. Since $0\in B$, we have $A\subset C$ and hence $|A|+|B|\leqq|C|+|\Delta C|$.

If $B+A\not\subset A$, $e$ may be chosen so as to make $B^*$ minimal as before.

The proof now divides into three cases.

*Case* I. For every $a$ in $A$, $a+H\subset A$.

In this case $A+H\subset A$ so that $H\subset\Delta A=\Delta C$. Hence

$$|A|+|B|=|A'|+|B'|\leqq|C'|+|H|\leqq|C|+|\Delta C|$$

follows from $P_2$, (1), $P_0$ and the last containment.

*Case* II. There is an $a$ in $A$ with $a+H\not\subset A$ and $(a+H)\cap A^*$ is empty.

In this case the theorem follows immediately from Lemma 2.

*Case* III. For every $a$ in $A$, either $a+H\subset A$ or $(a+H)\cap A^*$ is nonempty. Moreover, for some $a$ in $A$, $a+H\not\subset A$.

In this case we can show $A+\Delta K\subset A$. For any $a$ in $A$, if $a+H\subset A$, then $K$ is contained in the subgroup $H$, hence so is $\Delta K$ and thus $a+\Delta K\subset A$. If $a+H\not\subset A$, then there is an $a^*$ in $A^*\cap(a+H)$. By Lemma 3,

$$a + \Delta K \subset (a + H) \cap A + \Delta K = a^* + K + \Delta K = a^* + K \subset A,$$

which proves the assertion.

This implies that $\Delta K\subset\Delta A=\Delta C$, so that by Lemma 4

$$|(a + H) \cap A^*| \leqq |\Delta C|. \tag{2}$$

There is some $a$ in $A$ with $a+H\not\subset A$, so that Lemma 2 together with (2) now imply the theorem.

This statement of Kneser's theorem suggests the following conjectures for sets of nonnegative integers.

Let $A+B=C$. Let $H^{(n)}=\{x:c\in C, x+c\leqq n \text{ implies } x+c\in C\}$; then

$$\min_{m\leqq n}\frac{C(m)+H^{(n)}(m)}{m+1}\geqq\min_{m\leqq n}\frac{A(m)+B(m)}{m+1}.$$

Furthermore, it seems that $H^{(n)}$ may be replaced by

$$J^{(n)} = \{x:c \in C,\ c \leqq n \text{ implies } x + c \in C\}.$$

Either of these conjectures implies both Mann's theorem and Kneser's theorem for sets of integers.

## Bibliography

1. H. B. Mann, *Addition theorems: The addition theorems of group theory and number theory*, Interscience, New York, 1965. MR **31** #5854.

2832 S.W. Sam Jackson Park Road, Portland, Oregon 97201