COMPLEXES IN ABELIAN GROUPS

PETER SCHERK AND J. H. B. KEMPERMAN

Introduction. Let G be an abelian group of order $[G] \leqslant \infty$. Let $A = \{a\}$, $B = \{b\}, \ldots$ denote non-empty finite complexes in G. Let $[A]$ be the number of elements of A. Finally put

$$A + B = \{a + b\}.$$

If $[A] + [B] > [G]$, then **(7)** obviously $A + B = G$. From now on we shall assume

0.1 $$[A] + [B] \leqslant [G].$$

A well-known theorem by Cauchy and Davenport states that

0.2 $$[A + B] \geqslant [A] + [B] - 1$$

if G is cyclic of prime order **(1; 3; 4)**. But 0.2 need not hold true any longer if G is cyclic and $[G]$ is composite. However, Chowla **(2)** proved 0.2 for cyclic G's under an additional assumption.

Let k be a fixed integer with $k \geqslant 1$. We wish to prove

0.3 $$[A + B] \geqslant [A] + [B] - k$$

and related results under various additional conditions and for arbitrary abelian G's. All these conditions Γ, $\bar{\Gamma}$, $\Delta, \ldots$ will be empty if $[B] \leqslant k$.

Our results can be obtained by adaptations of Davenport's method **(3)**. However, we shall use a slightly different approach which is also related to Mann's **(7)** and to another paper by the authors (appearing immediately after the present one).

The Main Result

1. The Condition Γ_1. We first prove 0.3 for complexes A, B which satisfy the following

Condition $\Gamma_1(A, B)$:

(i) *If $[B] > k$ and if $\Gamma_1(A, B)$ holds, then there is an element b_0 in B such that*

1.1 $$A + B \not\subset A + b_0.$$

(ii) *$\Gamma_1(A, B)$ implies $\Gamma_1(A_2, B_2)$ for every pair of complexes A_2, B_2 such that*

1.2 $$b_0 \subset B_2 \subset B, \quad A \subset A_2,$$

1.3 $$[A_2] - [A] = [B] - [B_2],$$

and

1.4 $$A_2 + B_2 \subset A + B.$$

Received January 8, 1953; in revised form May 26, 1953.

https://doi.org/10.4153/CJM-1954-024-4 Published online by Cambridge University Press

Our statement is trivial for $[B] \leqslant k$. Suppose it is proved for $[B] \leqslant n - 1$ and let $[B] = n$ $(n > k)$. From 1.1 there is an a_0 in A such that

$$a_1 = a_0 + b_1 - b_0 \not\subset A$$

has solutions b_1 in B. Let $A_1 = \{a_1\}$ and $B_1 = \{b_1\}$. Since $b_0 \not\subset B_1$ we have

1.5 $$0 < [A_1] = [B_1] < [B].$$

Let $A_2 = A \cup A_1$ and let B_2 be the complement of B_1 in B. Thus 1.2 and 1.3 are satisfied and

1.6 $$0 < [B_2] < [B].$$

We now verify 1.4. Since $A + B_2 \subset A + B$, we have only to show that

1.7 $$A_1 + B_2 \subset A + B.$$

Let $a_1 \subset A_1$, $b_2 \subset B_2$. Thus $a_1 = a_0 + b_1 - b_0$. The definition of B_1 and $b_2 \subset B_2$ imply $a_0 + b_2 - b_0 \subset A$. Hence

$$\begin{aligned} a_1 + b_2 = (a_0 + b_1 - b_0) + b_2 &= (a_0 + b_2 - b_0) + b_1 \\ &\subset A + B_1 \subset A + B. \end{aligned}$$

This proves 1.7 and hence 1.4.

From 1.6 and our induction assumption, we have

1.8 $$[A_2 + B_2] \geqslant [A_2] + [B_2] - k.$$

Finally, 1.4, 1.8 and 1.3 yield

$$[A + B] \geqslant [A_2 + B_2] \geqslant [A_2] + [B_2] - k = [A] + [B] - k.$$

2. The Condition Γ_2. Our Condition Γ_1 is implied by

CONDITION $\Gamma_2([A], B)$:

(i) *If $k < [B] \leqslant [A]$, then there are two elements b_0 and b_1 in B such that*

2.1 $$[A](b_1 - b_0) \neq 0.$$

(ii) $\Gamma_2([A], B)$ *implies* $\Gamma_2([A] + [B] - [B_2], B_2)$ *for every subcomplex B_2 of B that contains b_0.*

It suffices to prove 1.1. Let $b_0 \subset B$ be arbitrary if $[B] > [A]$. Choose b_0 according to (i) if $k < [B] \leqslant [A]$. Suppose

2.2 $$a_1 = a + b - b_0 \subset A$$

for every a, b. If $[B] > [A]$, we keep a fixed and let b run through B. This would yield more than $[A]$ different elements of A. If $[B] \leqslant [A]$, we specialize $b = b_1$. If a runs through A, then so will a_1. Hence

$$\Sigma a = \Sigma a_1 = \Sigma(a + (b_1 - b_0) = \Sigma a + [A](b_1 - b_0)$$

or

$$[A](b_1 - b_0) = 0.$$

This contradicts 2.1. Thus 2.2 is false for some a, b. This implies 1.1.

https://doi.org/10.4153/CJM-1954-024-4 Published online by Cambridge University Press

3. Further specializations. Condition Γ_2 is certainly satisfied if each B_2 with

3.1 $$b_0 \subset B_2 \subset B$$

and

3.2 $$k < [B_2] \leqslant [A] + [B] - [B_2]$$

contains an element b such that

3.3 $$([A] + [B] - [B_2])(b - b_0) \neq 0.$$

This in turn is sure to be the case if the relation 3.3 has not less than $[B] - [B_2]+1$ solutions in B for each $[B_2]$ satisfying 3.2. We thus arrive at

CONDITION $\Gamma_3([A], B)$: *There is a b_0 in B such that the relation*

3.4 $$([A] + m)(b - b_0) \neq 0$$

has not less than $m + 1$ solutions b in B whenever

$$\max (0, \tfrac{1}{2}[B] - \tfrac{1}{2}[A]) \leqslant m \leqslant [B] - k - 1.$$

Condition Γ_3 is always satisfied if $[A]$ and $[B]$ are not too large. Suppose, e.g., that G has the type $(p_1^{\alpha_1}, \ldots , p_n^{\alpha_n})$ and that

3.5 $$[A] + [B] - k \leqslant \min (p_1, \ldots , p_n, [G] - k)$$

(some of the p_k's may be infinite). Then $[A] + m$ will be prime to the product of all finite p_k's and 3.4 will hold for each $b \neq b_0$. Thus 3.5 implies 0.3.

Let G be a finite cyclic group. Suppose there is a b_0 in B such that

3.6 $$b - b_0 \text{ is primitive for each } b \neq b_0.$$

Then, for $m < [B]$, 0.1 implies $[A] + m < [A] + [B] \leqslant [G]$. Hence each $b \neq b_0$ satisfies 3.4. Condition Γ_3 is satisfied, even if $k = 1$, and 0.2 holds. If we represent G by the cyclic group of residue classes (mod $[G]$), then 3.6 is equivalent to

3.7 $$(b - b_0, [G]) = 1 \text{ for each } b \neq b_0.$$

Chowla's theorem is identical with the observation that 0.1 and 3.7 imply 0.2. If $[G]$ is a prime number, then 3.7 is trivially satisfied and 0.2 follows from 0.1. This is the theorem of Cauchy and Davenport.

4. Comments. Suppose that for $k \geqslant 1$

4.1 $$[A + B] < [A] + [B] - k$$

and let $b_0 \subset B$. Then there exist two complexes A' and B' such that

4.2 $$A \subset A', \qquad b_0 \subset B' \subset B,$$

4.3 $$k < [B'] \leqslant [B],$$

4.4 $$[A'] - [A] = [B] - [B'],$$

4.5 $$A' + B' \subset A + B,$$

4.6 $$A' + B' - b_0 = A'.$$

In fact, we obtain such complexes A' and B' by iterating our construction of A_2 and B_2 (cf. §**1**) as often as possible, each time with b_0 as the basic element.

Let B^- be the set of elements $b' - b_0$ ($b' \subset B'$) and let B_0^- be the subgroup generated by B^-. Hence

4.7 $$k + 1 \leqslant [B'] = [B^-] \leqslant [B_0^-].$$

By 4.6, $A' + B^- = A'$. Because A' is finite, we have that B_0^- is finite and

4.8 $$A' + B_0^- = A'.$$

Thus A' consists of cosets of B_0^-. In particular, $[A'] = [A] + [B] - [B']$ will be a multiple of $[B_0^-]$. Therefore, putting $[B] - [B'] = m$,

$$([A] + m)(b - b_0) = 0$$

for each of the $[B'] = [B] - m$ elements in B'. Thus the relation

$$([A] + m)(b - b_0) \neq 0$$

has at most m solutions in B. By $k < [B'] \leqslant [B]$, we have

$$0 \leqslant m \leqslant [B] - k - 1.$$

Moreover, 4.6 implies $[B'] \leqslant [A'] = [A] + [B] - [B']$, that is,

$$m \geqslant -\tfrac{1}{2}[A] + \tfrac{1}{2}[B].$$

Consequently, if 4.1 holds, Condition Γ_3 cannot be true, which yields a second proof that Γ_3 implies 0.3.

Another consequence of 4.1 is:

$$A + B_0^- + b_0 \subset A' + B_0^- + b_0 = A' + b_0 \subset A' + B' \subset A + B.$$

Therefore:

The inequality 4.1 *implies, for each b_0 in B, the existence of at least k different elements $b_i \neq b_0$ in B such that the group B_0^- generated by the differences $b_i - b_0$ is finite and satisfies*

$$A + B_0^- + b_0 \subset A + B.$$

As an easy consequence of the special case $k = 1$, $0 \subset B \subset A$, $b_0 = 0$, we obtain a theorem due to Shepherdson (**8**, p. 85).

Variants

In the following, $A, B, \ldots$ will still be non-empty complexes in G. Their finiteness, however, and 0.1 will not necessarily be assumed. We wish to discuss some variants of §**1**. The analogues of §§**2–4** being rather obvious, only some of them will be stated.

https://doi.org/10.4153/CJM-1954-024-4 Published online by Cambridge University Press

5. The complex $\bar{A}$. Let $\bar{A}$ be the complement of A in G. In this section, $\bar{A}$ and B are assumed to be finite. Only the case $[G] = \infty$ will be of interest.

If $g \subset \overline{A + B}$, then $g - b \subset \bar{A}$ for any b. Hence

$$[\bar{A}] \geqslant [\overline{A + B}].$$

In particular, the finiteness of $\bar{A}$ implies that of $\overline{A + B}$. Also, *if*

5.1 $$[B] > [\bar{A}],$$

then $A + B = G$.

Proof. Let g be any element of G and let b range through B. From 5.1, not all of the $[B]$ elements $g - b$ can lie in $\bar{A}$. Thus $a = g - b \subset A$ for some b, that is, $g \subset A + B$.

Again, let k be a fixed integer with $k \geqslant 1$. The following analogue of §1 can now be stated:

Suppose

5.2 $$[B] \leqslant [\bar{A}].$$

Then

5.3 $$[\overline{A + B}] \leqslant [\bar{A}] - [B] + k$$

provided that $\bar{A}$ *and* B *satisfy some Condition* $\bar{\Gamma}$.

Condition $\bar{\Gamma}_1(\bar{A}, B)$:

(i) *If* $[B] > k$ *and if* $\bar{\Gamma}_1(\bar{A}, B)$ *holds true, then there is an element* b_0 *in* B *such that*

5.4 $$A + B \not\subset A + b_0.$$

(ii) $\bar{\Gamma}_1(\bar{A}, B)$ *implies* $\bar{\Gamma}_1(\bar{A}_2, B_2)$ *for every pair of complexes* A_2, B_2 *satisfying* 1.2, 1.4 *and*

5.5 $$[\bar{A}] - [\bar{A}_2] = [B] - [B_2].$$

The proof of the sufficiency of condition $\bar{\Gamma}_1(\bar{A}, B)$ is identical with the proof in §**1**. Only 1.3 has to be replaced by 5.5 and 1.8 by

$$[\overline{A_2 + B_2}] \leqslant [\bar{A}_2] - [B_2] + k.$$

We note that the left hand terms of 5.5 and 1.3 both count the number of those elements of A_2 that do not lie in A.

Condition $\bar{\Gamma}_2([\bar{A}], B)$ is obtained by replacing $[A]$ in Condition Γ_2 by $[\bar{A}]$ and $[A] + [B] - [B_2]$ by $[\bar{A}] - [B] + [B_2]$. In verifying this condition we use the fact that $\bar{A} + B \not\subset \bar{A} + b_1$ for some $b_1 \subset B$ implies 5.4 for some $b_0 \subset B$.

The following is an analogue of Γ_3.

Condition $\bar{\Gamma}_3$ $([\bar{A}], B)$: *There is a* b_0 *in* B *such that each of the relations*

5.6 $$([\bar{A}] - m)(b - b_0) \neq 0$$

has not less than $m + 1$ *solutions* b *in* B $(m = 0, 1, \ldots, [B] - k - 1)$.

6. Inversion and differences of complexes. In this section, A, B, C may be arbitrary complexes in G. They may be empty or infinite.

The *difference* $A - B$ of A and B is defined **(5)** to be the set of all those $c \subset G$ such that $c + B \subset A$. If $A \subset A'$ and $B \subset B'$ then

6.1 $$A - B' \subset A - B \subset A' - B.$$

Obviously

6.2 $$A + B \subset C \leftrightarrow A \subset C - B.$$

Another connection between sums and differences can be obtained by means of a concept essentially due to Khintchine **(6)**. Let i be any fixed element of G. The inversion $\tilde{A}$ of A with respect to i consists of all the elements $i - \bar{a}$ where $\bar{a} \subset \bar{A}$. Thus $(\tilde{A})^{\sim} = A$ and $[\tilde{A}] = [\bar{A}]$. We readily verify **(5)**

6.3 $$A - B = (\tilde{A} + B)^{\sim}, \quad A + B = (\tilde{A} - B)^{\sim}.$$

If $A + B \subset C$, then $\tilde{C} \subset (A + B)^{\sim} = \tilde{A} - B$ and hence from 6.2

6.4 $$B + \tilde{C} \subset \tilde{A}.$$

This is an analogue of Khintchine's inversion formula **(6)**.

7. The dual theorems. Formula 6.3 enables us to derive duals of §§**1**–**4** from §**5**.

Let C and B denote finite non-empty complexes in G. Put

7.1 $$A = \tilde{C}.$$

Then

7.2 $$C - B = (A + B)^{\sim},$$

7.3 $$[\bar{A}] = [C] < \infty \text{ and } [C - B] = [\overline{A + B}] < \infty.$$

If $[B] > [C]$, $C - B$ is empty. Furthermore, $[C] = [G]$ implies $C = C - B = G$ on account of $[B] > 0$.

7.1–7.3 enable us to translate §**5**. Let k be a fixed integer with $k \geqslant 1$.

Suppose

7.4 $$[B] \leqslant [C] < [G].$$

Then

7.5 $$[C - B] \leqslant [C] - [B] + k$$

provided that B and C satisfy a Condition Δ.

Condition $\bar{\Gamma}_1(\bar{A}, B)$ yields

CONDITION $\Delta_1(C, B)$:

(i) *If* $[B] > k$ *and if* $\Delta_1(C, B)$ *holds there is an element* b_0 *in* B *such that*

7.6 $$C + B \not\subset C + b_0.$$

(ii) $\Delta_1(C, B)$ *implies* $\Delta_1(C_2, B_2)$ *for every pair of complexes* C_2, B_2 *such that*

7.7 $$b_0 \subset B_2 \subset B, \quad C_2 \subset C,$$

7.8 $$[C] - [C_2] = [B] - [B_2],$$
and
7.9 $$C - B \subset C_2 - B_2.$$

Condition $\bar{\Gamma}_3$ leads to

CONDITION $\Delta_2([C], B)$: *There is a b_0 in B such that each of the relations*

7.10 $$([C] - m)(b - b_0) \neq 0$$

has not less than $m + 1$ solutions in B $(m = 0, 1, \ldots, [B] - k - 1)$.

If B and $\bar{C}$ are finite, we may obtain similar results for $[\overline{C - B}]$ applying **§1** rather than **§5**.

8. A condition on $A + B$. In the last sections of this paper, A and B denote again finite non-empty complexes in G which satisfy 0.1. Formula 6.4 suggests that the following variant of Γ_1 implies 0.3.

CONDITION $\Gamma_4(A, B)$:

(i) *If $[B] > k$ and if $\Gamma_4(A, B)$ holds, then there is an element b_0 in B such that*

8.1 $$(A + B) + B \not\subset (A + B) + b_0.$$

(ii) $\Gamma_4(A, B)$ *implies* $\Gamma_4(A, B_2)$ *for every complex B_2 such that*

8.2 $$b_0 \subset B_2 \subset B.$$

We wish to give a direct proof by induction. By 8.1, there is a $\bar{c}_0 \subset \overline{A + B}$ such that

8.3 $$c_1 + b_1 = \bar{c}_0 + b_0$$

has solutions $c_1 \subset A + B$, $b_1 \subset B$. Put $B_1 = \{b_1\}$, $C_1 = \{c_1\}$. Thus

8.4 $$0 < [C_1] = [B_1] < [B].$$

Let B_2 be the complement of B_1 in B and let C_2 denote **(3)** the complement of C_1 in $A + B$. From 8.4,

8.5 $$[C_2] = [A + B] - [B] + [B_2].$$

We readily verify (cf. 1.7) that

8.6 $$A + B_2 \subset C_2.$$

Since $b_0 \subset B_2 \subset B$ and $[B_2] < [B]$, our induction assumption implies

8.7 $$[A + B_2] \geqslant [A] + [B_2] - k.$$

Finally, 8.5, 8.6 and 8.7 yield 0.3.

9. Final corollaries. A condition which does not involve $A + B$ is

CONDITION $\Gamma_5([A], B)$:

(i) *If* $[B] > k$ *and if* $\Gamma_5([A], B)$ *holds, there are two elements* b_0, b_1 *in* B *such that*

9.1 $$([A] + [B] - k - 1)(b_1 - b_0) \neq 0.$$

(ii) $\Gamma_5([A], B)$ *implies* $\Gamma_5([A], B_2)$ *for every subcomplex* B_2 *of* B *that contains* b_0.

Proof. Suppose there exists a smallest positive integer n such that 0.3 is false for $[B] = n$. Then $n > k$ and there are two complexes A, B which satisfy Condition $\Gamma_5([A], B)$ and $[B] = n$ but not 0.3. Thus

9.2 $$[A + B] = [A] + [B] - k - 1.$$

On account of part (i) of Condition Γ_5, the relation

9.3 $$[A + B](b_1 - b_0) \neq 0$$

then has solutions b_0, b_1 in B. This easily implies (cf. §**2**) that b_0 is a solution of 8.1. Therefore, we can construct a pair of sets B_2, C_2 for which 8.4, 8.5, and 8.6 hold. Moreover, by induction, 8.7 is true. This yields 0.3, contradicting 9.2.

The following is a special case of Γ_5.

CONDITION $\Gamma_6([A], B)$: *There is a* b_0 *in* B *such that*

9.4 $$([A] + m)(b - b_0) = 0$$

has not more than $m + k$ *solutions* b *in* B $(m = 0, 1, \ldots, [B] - k - 1)$.

In a similar way, more conditions $\bar{\Gamma}$ and Δ can be derived.

REFERENCES

1. A. L. de Cauchy, *Recherches sur les nombres*, Œuvres (2nd series, Paris, 1882), vol. 1, 39–63.
2. I. Chowla, *A theorem on the addition of residue classes*, Proc. Indian Acad. Sci., *2* (1935), 242–243.
3. H. Davenport, *On the addition of residue classes*, J. London Math. Soc., *10* (1935), 30–32.
4. ———, *A historical note*, J. London Math. Soc., *22* (1947), 100–101.
5. H. Hadwiger, *Minkowskische Addition und Subtraktion beliebiger Punktmengen und die Theoreme von Erhard Schmidt*, Math. Zeitschr., *53* (1950), 210–218.
6. A. Khintchine, *Zur additiven Zahlentheorie*, Matem. Sbornik, *39* (1932), 27–34.
7. H. B. Mann, *On products of sets of group elements*, Can. J. Math., *4* (1952), 64–66.
8. J. C. Shepherdson, *On the addition of elements of a sequence*, J. London Math. Soc., *22* (1947), 85–88.

University of Saskatchewan and
University of Southern California

Purdue University