Proc. Camb. Phil. Soc. (1963), **59**, 559
Printed in Great Britain

A combinatorial problem in Abelian groups

BY KENNETH ROGERS
Department of Mathematics, University of California at Los Angeles

Communicated by J. W. S. CASSELS

(*Received* 21 *December* 1962)

1. Let α be a prime element of the ring of integers of an algebraic number field, R. Mr C. Sudler verbally raised the question as to how many prime ideal factors α can have. This is equivalent to a problem on the group of ideal classes of R, as we now show. If there is a prime $\alpha = p_1 p_2 \dots p_k$, where the prime ideal p_i is in the ideal class P_i, then $P_1 P_2 \dots P_k$ equals the identity class, but no subproduct has this property. The converse holds since every ideal class contains prime ideals. So the problem is equivalent to one on finite Abelian groups, which we now write additively.

For a finite Abelian group G, find the largest integer h such that there exists a sequence $a_1, \dots, a_h$ of elements of G with no partial sum equal to zero, except the empty sum. We shall call such sequences *admissible*. The answer to Sudler's question is then $K = h + 1$.

LEMMA 1. *For all G we have $h < \operatorname{ord} G$. If $G = G_1 \oplus G_2$ and the corresponding numbers are h, h_1, h_2 then $h_1 + h_2 \leqslant h \leqslant h_1 h_2 + h_1 + h_2$.*

Proof. The admissible sequence $\{a_1, a_2, \dots, a_h\}$ yields the h distinct non-zero elements $a_1, a_1 + a_2, \dots, a_1 + \dots + a_h$ and hence $h < \operatorname{ord} G$.

If $\{a_1, \dots, a_{h_1}\}$ is an admissible sequence of G_1 and $\{b_1, \dots, b_{h_2}\}$ an admissible sequence of G_2 then $\{(a_1, 0), \dots, (a_{h_1}, 0), (0, b_1), \dots, (0, b_{h_2})\}$ is an admissible sequence of G, and hence $h_1 + h_2 \leqslant h$.

If G contained an admissible sequence of length $(h_1 + 1)(h_2 + 1)$ then we could divide it into $h_2 + 1$ disjoint subsequences of length $h_1 + 1$. In each of these subsequences there would exist a sum that lies in $\{0\} \oplus G_2$. Since there are $h_2 + 1$ such sums, there is a sum of them which is 0. Hence $h < (h_1 + 1)(h_2 + 1)$.

For Z_n, the cyclic group of order n, we have a complete characterization of maximal admissible sequences.

THEOREM 1. *All maximal admissible sequences for Z_n are of the form $a_1, \dots, a_{n-1}$ with $a_1 = a_2 = \dots = a_{n-1} =$ generator of Z_n.*

Proof. By Lemma 1, $h = n - 1$ in this case, so we need only show all a_i are equal. If $a_1 \neq a_2$, then the sums $a_1, a_1 + a_2, \dots, a_1 + \dots + a_{n-1}, a_2$ are all distinct and non-zero, which is not possible, by cardinality.

Note that we cannot expect such a simple description in the non-cyclic cases, since if $a_1, \dots, a_h$ is admissible, then so is $a_1, \dots, a_{h-1}, -\sum_{i=1}^{h} a_i$. Combining Theorem 1 and Lemma 1 we get

COROLLARY. *Let $G = Z_{e_1} \oplus Z_{e_2} \oplus \dots \oplus Z_{e_s}$ where $e_1 \mid e_2 \mid \dots \mid e_s$ so that these are the elementary divisors of G, then*

$$h \geqslant e_1 + \dots + e_s - s. \tag{1}$$

https://doi.org/10.1017/S0305004100037221 Published online by Cambridge University Press

We have shown that equality holds in (1) for $s = 1$ and we shall show that equality holds for $s = 2$ and $e_1 = 2^l 3^m 5^n$.

2. We now consider $Z_{e_1} \oplus Z_{e_2}$ and wish to reduce to the case of $Z_p \oplus Z_p$, where p is any prime. The method used here requires two theorems which we conjecture in general.

C_1: *Every sequence of length* $e_1 + e_2 - 1$ *from* $Z_{e_1} \oplus Z_{e_2}$ *has a zero subsum.*

C_2: *Every sequence of length* $2e_1 + e_2 - 2$ *from* $Z_{e_1} \oplus Z_{e_2}$ *has a zero sum of length at most* e_2.

In this connexion we mention a result of Erdős, Ginzburg and Ziv (1) to the effect that from a sequence of length $2n-1$ from Z_n we can pick a zero subsum of length n. We shall now show that C_1 and C_2 hold for $Z_{e_1} \oplus Z_{e_2}$ if they hold for all $Z_p \oplus Z_p$ with $p | e_1$.

THEOREM 2. *If* C_1 *and* C_2 *hold for* $Z_a \oplus Z_a$, *then they hold for* $Z_a \oplus Z_{ab}$, *where* $b > 1$.

Proof. Map $Z_a \oplus Z_{ab}$ homomorphically onto $Z_a \oplus Z_a$ by $(x, y) \to (x, by)$, so the kernel is a Z_b. For C_1, start with a sequence of length $(b+1)a - 1$: in the $Z_a \oplus Z_a$ image, we apply C_2 to 'peel off' chains of length at most a, with zero sum, $b-1$ times. After this, we apply C_1 to the remaining $2a-1$ or more elements, giving in all a total of b disjoint subchains each having a sum in a certain Z_b. Now use Theorem 1. The same method works for C_2: start with $(b+2)a - 2$ elements and peel off b chains, each of length at most a and with sum in Z_b. This can be done, by C_2 on $Z_a \oplus Z_a$, since

$$(b+2)a - 2 - (b-1)a = 3a - 2.$$

THEOREM 3. *If* C_1 *and* C_2 *hold for* $Z_a \oplus Z_a$ *and* $Z_b \oplus Z_b$, *then* C_1 *and* C_2 *hold for* $Z_{ab} \oplus Z_{ab}$.

Proof. The homomorphism $(x, y) \to (bx, by)$ maps $Z_{ab} \oplus Z_{ab}$ onto $Z_a \oplus Z_a$, with kernel $Z_b \oplus Z_b$. From a chain of length $2ab - 1$ from $Z_{ab} \oplus Z_{ab}$, we get $2b-2$ disjoint chains of length at most a and sums in the kernel, and lastly a chain with sum in the kernel, by the use of C_2 and C_1 for $Z_a \oplus Z_a$. Now use C_1 for $Z_b \oplus Z_b$ on the $2b-1$ blocks just found. Similarly for proving C_2: now the length is $3ab - 2$, so $3b-2$ blocks with sums in $Z_b \oplus Z_b$ and lengths at most a each can be found.

COROLLARY. *To prove* C_1 *and* C_2 *for* $Z_m \oplus Z_{mn}$, *where* $m = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$, *it is enough to prove* C_1 *and* C_2 *for* $Z_p \oplus Z_p$, *with* $p = p_1, \dots, p_k$.

In the next section we verify C_1 and C_2 for $p = 2, 3, 5$.

3. THEOREM 4. C_1 *and* C_2 *hold for* $Z_2 \oplus Z_2$ *and* $Z_3 \oplus Z_3$.

Proof. For $Z_2 \oplus Z_2$: since an admissible chain contains neither zero nor pairs $\{a, -a\} = \{a, a\}$, it cannot be of length 3, because $(a, b, a+b)$ has zero sum. Similarly, any chain of length 4 contains zero or a repetition, so C_2 holds. Indeed, since the direct sum of n groups Z_2 can be considered an n-dimensional vector space over $GF(2)$ we clearly have $h = n$. The analogue to C_2 is also trivial in this case, since the minimal length of a sequence from $GF(2^n)$ which must contain 0 or a pair (a, a) is clearly 2^n.

For $Z_3 \oplus Z_3$: this group has 4 pairs of the form $\pm a$, hence an admissible sequence of length 5 would contain a repetition and be of the form x, x, u, v, w. By mod x considerations, we know that $\{u, v, w\}$ has a subsum within the x-group which, together with the x, x, has a zero sum. To prove C_2, assume we had a sequence of length 7, all of whose triples are admissible. Proceeding as before, we come to the form x, x, y, y, z, z, w, where any two distinct letters span the group. Since x, y, z are dependent over

https://doi.org/10.1017/S0305004100037221 Published online by Cambridge University Press

$GF(3)$, we have $z = ax + by$ with $a, b \in \{1, 2\}$. But then $(x, x, y, y, ax + by, ax + by)$ spans every group element as a sum of 0, 1 or 2 elements of the sequence; hence w and at most two others form a zero sum.

THEOREM 5. *A sequence of length 9 from $Z_5 + Z_5$ contains a subsequence whose sum is zero.*

Proof. This group is the union of six subgroups of order 5, so that the sequence contains at least two members in the same Z_5.

Case (i). *There are four elements in a Z_5.* If a_1, a_2, a_3, a_4 are in a Z_5, then since some subsum of $(a_5, \ldots, a_9)$ is in this Z_5, we get the right number to ensure a zero sum.

Case (ii). *The elements a_1, a_2, a_3 are in a Z_5.* A more careful use of the argument in (i) shows that we must have $a_1 = a_2 = a_3 =$ all sums in $(a_4, \ldots, a_9)$ which lie in this subgroup. Thus, if any three a_i are in a common Z_5, they must be equal. Write $a = a_1 = a_2 = a_3$ and consider the rest mod a.

(1) $a_4 \equiv a_5 \equiv \ldots \equiv a_9 \pmod{a}$. In this case the sum of any five of these six elements must be equal to a and therefore $a_4 = a_5 = \ldots = a_9$ leading back to case (i).

(2) $a_4 \equiv a_5 \equiv a_6 \equiv a_7 \not\equiv a_8 \pmod{a}$. Here the sum of a_8 with fewer than four terms from $\{a_4, a_5, a_6, a_7\}$ must be equal to a and hence $a_4 = a_5 = a_6 = a_7$ leading back to case (i).

(3) $a_4 \equiv -a_5 \pmod{a}$. Since $a_4 + a_5 \in \langle a \rangle$, the group generated by a, no sum from $\{a_6, a_7, a_8, a_9\}$ can lie in $\langle a \rangle$. But then, by Theorem 1, we have $a_6 \equiv a_7 \equiv a_8 \equiv a_9 \pmod{a}$ which is one of the previous cases.

We are therefore left with the only possibility.

(4) $a_4 \equiv a_5 \equiv a_6 \pmod{a}$, $a_7 \equiv a_8 \equiv a_9 \pmod{a}$, $a_4 \not\equiv \pm a_7 \pmod{a}$. Here the sum of two or three elements from $\{a_4, a_5, a_6\}$ with each element of $\{a_7, a_8, a_9\}$ must be a and we therefore get $a_4 = a_5 = a_6$ and $a_7 = a_8 = a_9$. The sequence therefore is $a, a, a, b, b, b, c, c, c$ where $c \not\equiv \pm a \pmod{b}$ and $c \not\equiv \pm b \pmod{a}$. Thus $c = \pm 2a \pm 2b$ and 0 is the sum of c with 2 or 3 a's and 2 or 3 b's.

Case (iii). *No 3 terms in a common Z_5.* We have mentioned already that there must be 2 terms, say a_1 and a_2, in a Z_5.

(1) $a_1 \not\equiv a_2$. We may write $a_1 = a$, $a_2 = 2a$. Then all sums from $\{a_3, \ldots, a_9\}$ which lie in $\langle a \rangle$ must be equal to a and there cannot be two disjoint such sums. If $a_3 + a_4 = a$ then $\{a_5, \ldots, a_9\}$ has a sum in $\langle a \rangle$ which is impossible. If $a_3 + a_4 + a_5 = a$ then $a_6 \equiv a_7 \equiv a_8 \equiv a_9 \pmod{a}$ and since we do not have $a_3 \equiv a_4 \equiv a_5 \pmod{a}$ the sum of fewer than 4 elements from $\{a_6, a_7, a_8, a_9\}$ with one element from $\{a_3, a_4, a_5\}$ must be a. Hence $a_6 = a_7 = a_8 = a_9$ which is case (i). If no 3 terms of $\{a_3, \ldots, a_9\}$ have a sum in $\langle a \rangle$ then we must have 6 terms congruent (mod a). Since the sum of 5 of these is a they are all equal which is case (i).

(2) *Unequal a_i are from distinct subgroups.* In this case we have the form $a, a, b, b, c, c, a_7, a_8, a_9$ where a, b and c are from 3 of the 6 subgroups, while the last 3 are of form d, d, e or d, e, f, where d, e and f generate the other 3 subgroups. Now, the pairwise independent elements a, b, c form a dependent set and the possible l, m, n with $la = bm + cn$ reduce to

$$111,\ 211,\ 112,\ 212,\ 122,$$

since the other cases give zero sums or reduce to one of these. But 211 gives $a = 3(b + c)$, and so $a + 2b + 2c = 0$; while 122 gives $2a + b + c = 2(2b + 2c) + b + c = 0$. Also 112 and

https://doi.org/10.1017/S0305004100037221 Published online by Cambridge University Press

212 are equivalent, as $2a = b + 2c$ implies that $c = a + 2b$. This leaves the cases $a = b + c$ and $a = b + 2c$.

If $a = b + c$, we compute the partial sums of $(b, b, c, c, b + c, b + c)$ and infer that, for $(a_1, \ldots, a_9)$ to be admissible, the partial sums of (a_7, a_8, a_9) must be among

$$\{3b,\ 4b,\ 3c,\ 4c,\ b + 4c,\ c + 4b\}.$$

Since no 3 of $a_1, \ldots$ are in a Z_5, the last triple must take values only from $\{\pm(b + 4c)\}$ and take both values, with zero sum.

If $a = b + 2c$, then since $(b, b, c, b + 2c, b + 2c)$ has all of b, $2b$, $3b$, $4b$ as partial sums, the elements c, a_7, a_8, a_9 cannot 'span' any element in $\langle b \rangle$, hence they must all be of the form $c + nb$, and we recall that a_7, a_8, a_9 are unequal to c. However, all elements of form $4c + nb \neq 4c$ are among the partial sums of $(b, b, c, c, b + 2c, b + 2c)$, so again we have a zero sum.

This completes case (iii) and proves Theorem 5. To complete the proofs of the results announced in § 1, it is only necessary to show that every sequence of length 13 from $Z_5 + Z_5$ has a zero partial sum of length at most 5. This we have done, but the details are even more tedious than above. The only new technique is the use made in one case of the result (1) already mentioned. In any case it shows no promise of generalization to $Z_p \oplus Z_p$.

4. There is a point in § 1 which we want to amplify: we saw that for the group $Z_{e_1} \oplus \ldots \oplus Z_{e_s}$ we have

$$h \geqslant \sum_{i=1}^{s} (e_i - 1),$$

whether or not the e_i are the elementary divisors. Since it is natural to ask if $\sum_{i=1}^{s} (e_i - 1)$ is maximized by the canonical representation, we now prove this is so.

THEOREM 6. *If* $Z_{d_1} \oplus \ldots \oplus Z_{d_t} \cong Z_{e_1} \oplus \ldots \oplus Z_{e_s}$, *where* $e_1, e_2, \ldots, e_s$ *are the elementary divisors, but* $d_1, \ldots, d_t$ *are not, then*

$$\sum_{j=1}^{t} (d_j - 1) < \sum_{i=1}^{s} (e_i - 1).$$

Proof. Assume that $d_i < d_j$: then $Z_{d_i} \oplus Z_{d_j} = Z_{(d_i, d_j)} \oplus Z_{[d_i, d_j]}$. But

$$d_i + d_j \leqslant (d_i, d_j) + [d_i, d_j]$$

with equality only for $d_i | d_j$ since $x + d_i d_j / x$ is a decreasing function for $x^2 < d_i d_j$. Thus, if $d_1, \ldots, d_t$ are not elementary divisors the sum $\Sigma(d_j - 1)$ can be increased, and the maximum must be attained for the elementary divisors.

5. It is clear that to disprove C_1 one must go to groups of high order. Basil Gordon and I have verified the analogue of C_1 for a few groups such as $Z_2 \oplus Z_2 \oplus Z_4$, so C_1 is good for some 3-generator groups beyond $GF(8)^+$. Much remains to be done.

In conclusion I thank Basil Gordon, T. S. Motzkin and Ernst Straus for helpful conversations.

REFERENCE

(1) ERDŐS, P., GINZBURG, A. and ZIV, A. Theorem in the additive number theory. *Bull. Res. Council Israel, Sect. F*, **10** (1961), F1.

https://doi.org/10.1017/S0305004100037221 Published online by Cambridge University Press