SOME PROBLEMS ON SPLITTINGS OF GROUPS. II
SÁNDOR SZABÓ
(Communicated by Bhama Srinivasan)
To Sherman Stein on his 60th birthday

ABSTRACT. If $G$ is an additive abelian group, $S$ is a subset of $G$, $M$ is a set of nonzero integers, and if each element of $G \setminus \{0\}$ is uniquely expressible in the form $ms$, where $m \in M$ and $s \in S$, then we say that $M$ splits $G$. A splitting is nonsingular if every element of $M$ is relatively prime to the order of $G$; otherwise it is singular. In this paper we discuss the singular splittings of cyclic groups of prime power orders and the direct sum of isomorphic copies of groups.

1. Introduction. Let $G$ be a finite abelian group written additively and let $M$ be a set of nonzero integers. If there exists a subset $S$ of $G$ such that each element of $G \setminus \{0\}$ is uniquely expressible in the form $ms$, where $m \in M$ and $s \in S$, then we say that the multiplier set $M$ splits $G$ with splitting set $S$ and write $G \setminus \{0\} = MS$. If $|S| = n$, then we say that $M$ $n$-splits $G$.

We will say that $M$ $n$-packs $G$ if the elements $ms$ are distinct and nonzero, where $m \in M$, $s \in S$, and $|S| = n$. Similarly, we will speak of an $n$-covering of $G$. Namely, $M$ $n$-covers $G$ if the elements $ms$ cover $G \setminus \{0\}$, where $m \in M$, $s \in S$, and $|S| = n$.

When the multiplier set has the form $M = \{1, \ldots, k\}$ or $M = \{-k, \ldots, -1, 1, \ldots, k\}$, questions about $n$-splitting, $n$-covering, and $n$-packing grow out of problems on tiling, covering, and packing $n$-space by certain star bodies, the so-called crosses and semicrosses. See [7, 9, or 12], for instance.

In this paper, which is a sequel to [14], we will examine packing and splitting of finite abelian groups. All groups will be assumed finite and abelian.

2. Packings. As in [12], $g(k, n)$ and $h(k, n)$ will denote the order of the smallest group which has an $n$-packing by $M = \{1, \ldots, k\}$ and $M = \{-k, \ldots, -1, 1, \ldots, k\}$ respectively. Obviously, $kn + 1 \leq g(n, k)$ and $2kn + 1 \leq h(k, n)$. The fact that the fractions $(kn + 1)/g(n, k)$ and $(2kn + 1)/h(k, n)$ equal the density of the densest integer lattice packing by crosses and semicrosses shows the significance of these functions. In [6] it was proved that, for $n \geq 3$,

$$\lim_{k \to \infty} g(k, n)k^{-3/2} = 2 \cos(\pi/n),$$

and in [12] it was proved that, for $n \geq 2$,

$$\lim_{k \to \infty} h(k, n)k^{-2} = 1.$$
We will prove the following result, which was obtained in [12] with the extra assumption that \( M = \{1, \ldots, k\} \) splits two groups of prime order.

**THEOREM 2.1.** \( \lim_{n \to \infty} \frac{(kn + 1)}{g(k, n)} = 1 \).

**PROOF.** Let \( u = \frac{k}{v + 1} \), where \( v \geq 1 \), and denote by \( C(r) \) the additive group modulo \( r \). We prove that \( M = \{1, \ldots, k\} \) \((u - 1)\)-packs \( C(k) \oplus C(u) \) with packing set \( S = \{(1, t) : 1 \leq t \leq u - 1\} \).

Indeed, from \( m(1, t) = (0, 0) \), \( m \in M \), it follows that \( m \equiv 0 \) (mod \( k \)) and \( mt \equiv 0 \) (mod \( u \)) and so \( u | mt \). Since \( m \) is relatively prime to \( u \), it follows that \( u | m \). This is a contradiction because \( 1 \leq m \leq k \) and \( k < u \). Next assume that \( m(1, t) = m'(1, r) \), where \( m, m' \in M \) and \( 1 \leq t, r \leq u - 1 \)—that is, \( m \equiv m' \) (mod \( k \)) and \( mt \equiv m'r \) (mod \( u \)). Thus \( k|(m - m') \). Since \( -k + 1 \leq m - m' \leq k - 1 \), we have \( m = m' \). Using the second congruence we have \( u|m(t - r) \). We know \( m \) is relatively prime to \( u \) and so \( u|(t - r) \). Since \( -u + 2 \leq t - r \leq u - 2 \), it follows that \( t = r \). This proves that \( g(k, u - 1) \leq ku \).

Since the inequality \( kn + 1 \leq g(k, n) \) is trivial, to prove that

\[
\lim_{n \to \infty} \frac{g(k, n)}{(kn + 1)} = 1
\]

it is sufficient to prove that \( g(k, n) \leq k(n + k!) \). This inequality holds because there exists a positive integer \( v \) such that \( k!(v - 1) < n < k!v \). Using this and \( g(k, u - 1) \leq ku \) we have

\[
g(k, n) \leq g(k, k!v) \leq k(k!v + 1) \leq k(n + k!).
\]

In [10] S. K. Stein proved that \((k + 1)^2 \leq h(k, n)\) for \( n \geq 2 \). The next result gives an improvement of this.

**THEOREM 2.2.** \( \min\{(k + 1)(2k + 1), (k + 1)(n - k - 1)\} \leq h(k, n) \) for \( n \geq 2 \).

**PROOF.** We use an idea in [13]. Let \( G \) be a finite abelian group and suppose \( M = \{-k, \ldots, -1, 1, \ldots, k\} \) \( n \)-packs \( G \) with packing set \( S = \{s_1, \ldots, s_n\} \). Let the integer \( t \) satisfy the inequality \((k + 1)(t - 1) \leq |G| < (k + 1)t \). First we shall show that for each integer \( i, 2 \leq i \leq n \), there exist integers \( x_i, y_i \) such that \( k + 1 \leq x_i \leq t - 1 \), \( |y_i| \leq k \), and \( x_is_i + y_is_i = 0 \).

For simplicity let \( i = 2 \). Consider the elements \( a_1s_1 + a_2s_2 \), where \( 0 \leq a_1 \leq t - 1 \) and \( 0 \leq a_2 \leq k \). The number of these elements is greater than \(|G|\). So, according to the pigeonhole principle, there exist \((a_1, a_2)\) and \((a_1', a_2')\) for which \((a_1, a_2) \neq (a_1', a_2')\) and \( a_1s_1 + a_2s_2 = a_1's_1 + a_2's_2 \). We may assume that \( a_1' \leq a_1 \).

Let \( x_2 = a_1 - a_1' \) and \( y_2 = a_2 - a_2' \). Then \( x_2s_1 + y_2s_2 = 0 \), where \((x_2, y_2) \neq (0, 0)\) and \( 0 \leq x_2 \leq t - 1 \), \( |y_2| \leq k \). Finally, \( x_2s_1 = -y_2s_2 \) shows that \( 0 \leq x_2 \leq k \) is impossible.

Distinguish two cases depending on whether one of the \( y_i \)'s is 0. If all \( y_i \) differ from zero then the \( x_i \)'s are distinct for \( 2 \leq i \leq n \). Indeed, from \( x_i = x_j, x_is_i + y_is_i = 0, \) and \( x_js_j + y_js_j = 0 \) it follows that \( y_is_i = y_js_j \), which is a contradiction unless \( i = j \). From the relationship \( \{x_2, \ldots, x_n\} \subseteq \{k + 1, \ldots, t - 1\} \) we have \( n - 1 \leq t - 1 - k \), that is, \( n + k - 1 \leq t - 1 \). Hence

\[
(k + 1)(n + k - 1) \leq (k + 1)(t - 1) \leq |G|.
\]

If \( y_i = 0 \), then \( x_is_i = 0 \). Let the order of \( s_1 \) be \( |s_1| \). Since \( x_i \neq 0 \), \( |s_1||x_i| \). Thus \( |s_1| \leq x_i \leq t - 1 \). Observe that the elements \(-ks_1, \ldots, -s_1, 0, s_1, \ldots, ks_1\)
are distinct. Consequently, $2k + 1 \leq |s_1|$. Comparing our inequalities, we have $2k + 1 \leq t - 1$. Hence

$$(k + 1)(2k + 1) \leq (k + 1)(t - 1) \leq |G|.$$ 

This completes the proof.

REMARKS. Since $(k + 1)(2k + 1) \leq (k + 1)(n + k - 1)$ if and only if $n \geq k + 2$, Theorem 2.2 can be stated as follows

If $2 \leq n \leq k + 1$, $h(k, n) \geq (k + 1)(n + k - 1)$; for $n \geq k + 2$, $h(k, n) \geq (k + 1)(2k + 1)$.

When $n = k + 2$ the two bounds coincide.

When $n = 3$ this theorem provides $k^2 + 3k + 1 \leq h(k, 3)$. On the other hand, according to [10], $h(k, 3) \leq k^2 + 3k + 3$.

3. Splitting of cyclic p-groups. It is convenient to distinguish different types of splittings. If $M$ splits $G$ and each element of $M$ is relatively prime to the order of $G$ then we speak of a nonsingular splitting; otherwise the splitting is called singular.

If for each prime divisor of $|G|$ some element of $M$ is divisible by $p$ then we call the splitting purely singular.

Nonsingular splittings are intimately connected with exact sequences. Namely, as proved in [3], if

$${\{0\} \rightarrow G \rightarrow G' \rightarrow G'' \rightarrow \{0\}}$$

is an exact sequence of finite abelian groups and $M$ splits $G$ and $G''$ and the splitting of $G$ is nonsingular, then $M$ splits $G'$. In the opposite direction [5] proved that if $M$ splits $G'$ and $G''$, then it splits $G$. Using these facts we can see that $M$ splits $G$ nonsingularly if and only if it splits $C(p)$ for each prime divisor $p$ of $|G|$. It was proved in [1] that if $G = \bigoplus_{i=1}^{n} C(p_i)$, $p_i$ is a prime, and $n \geq 2$, then any splitting of $G$ is nonsingular; and it was conjectured that every splitting of a noncyclic $p$-group is nonsingular. This conjecture was proved in [5].

The next step is to examine splittings of $C(p^t)$, $t \geq 2$. As is shown in [7] $M = \{1, \ldots, p-1\}$ splits $C(p^2)$ with splitting set $S = \{1, p+1, 2p+1, \ldots, (p-1)p+1\}$. Note that either $M$ or $S$ may be viewed as the multiplier set. With $M$ as the multiplier set, the splitting is nonsingular, but with $S$ taken as the multiplier set the splitting is singular. However in [1] splitting of $C(2^t)$, for even $t \geq 4$, were constructed in which both $M$ and $S$ contain even elements. For instance, $\{1, -1, 2\}$ splits $C(16)$ with splitting set $\{1, 3, 5, 7, 4\}$. Let us call a splitting of a cyclic group $C(n)$ doubly singular if both the multiplier set and the splitting set contain elements not relatively prime to $n$. Thus $C(2^t)$ can have a double singular splitting. However, we will prove that if $p$ is an odd prime then $C(p^t)$ has no doubly singular splittings. Thus, if $C(p^t) \setminus \{0\} = MS$, either $M$ or $S$ contains only of elements relatively prime to $p$. If $S$ is that set, say, and is viewed as the multiplier set, then the splitting is nonsingular and $S$ splits $C(p)$.

We will use the notion of factorization of a finite abelian group by two of its subsets. If $A$ and $B$ are subsets of the abelian group $G$ and if each $g$ in $G$ is uniquely expressible in the form $g = a + b$, $a \in A$, $b \in B$, then we say that $G$ is factored by its subsets $A$ and $B$. It will be assumed that $0 \in A \cap B$. We will speak of an $m$-factorization of $G$ if each $g$ in $G$ is expressible in the form $g = a + b$, $a \in A$, $b \in B$ precisely $m$ times. Moreover, we will permit $A$ and $B$ to have multiple
elements, that is, \( A \) and \( B \) may be viewed as sequences in \( G \) with repeated values permitted.

**Theorem 3.1.** If \( p \) is a prime, \( 1 \le t, m < p \), and \( C(p^tm) = A + B \) is a factorization, then either \( A \) or \( B \) contains at least two elements from the same coset modulo the subgroup of order \( p \).

**Proof.** Let \( H \) be the subgroup of order \( m \) and let \( K \) be the subgroup of order \( p \). Let \( G \) be the factor group \( C(p^tm)/H \), which has order \( p^t \). The factorization \( C(p^tm) = A + B \) induces an \( m \)-factorization of \( G \), \( G = \overline{A} + \overline{B} \), where \( \overline{A} = \{ a + H : a \in A \} \), \( \overline{B} = \{ b + H : b \in B \} \), with repetitions counted.

Now, \( G \) is isomorphic to the cyclic group \( C(p^t) \) and the \( m \)-factorization \( G = \overline{A} + \overline{B} \) corresponds to an \( m \)-factorization \( C(p^t) = A^* + B^* \). Introduce the polynomials

\[
A^*(x) = \sum_{a^* \in A^*} x^{a^*} \quad \text{and} \quad B^*(x) = \sum_{b^* \in B^*} x^{b^*}.
\]

The coefficients are in the range \([0, m]\). Moreover, because \( A \) and \( B \) were normalized, the constant terms are not 0. From the \( m \)-factorization it follows that

\[
A^*(x)B^*(x) \equiv m(1 + x + \cdots + x^{p^t-1}) \pmod{1 - x^{p^t}}.
\]

Denote by \( F_n(x) \) the \( n \)-th cyclotomic polynomial. Since \( F_{p^t}(x) \) is irreducible over the field of rational numbers, it divides \( A^*(x) \) or \( B^*(x) \). Without loss of generality assume that \( F_{p^t}(x) \) divides \( A^*(x) \), that is,

\[
A^*(x) = F_{p^t}(x)D(x) = (1 + x^{p^t-1} + \cdots + x^{(p-1)p^{t-1}})D(x).
\]

Since the degree of \( A^*(x) \) is less than \( p^t \) and the degree of \( F_{p^t}(x) \) is \( p^t - p^{t-1} \), it follows that the degree of \( D(x) \) is less than \( p^{t-1} \).

Consequently, the monomials \( x^0, x^{p^t-1}, x^{2(p^t-1)}, \ldots, x^{(p-1)p^{t-1}} \) occur in \( A^*(x) \) with nonzero coefficients. Thus \( A^* \) contains the subgroup of order \( p \). This means that \( \overline{A} \) contains the subgroup of order \( p \), that is, there are elements \( a_1, a_2, \ldots, a_p \in A \) such that \( a_1 + H, a_2 + H, \ldots, a_p + H \) form the subgroup of \( G \) of order \( p \). Let \( K = \{ k_1, \ldots, k_p \} \). Then \( k_1 + H, k_2 + H, \ldots, k_p + H \) is also a subgroup of order \( p \) (since \( K \cap H = \{ 0 \} \)). Thus \( a_1 + H, a_2 + H, \ldots, a_p + H \) is a permutation of \( k_1 + H, k_2 + H, \ldots, k_p + H \). For convenience, reindex the \( k_i \)'s so that \( a_i + H = k_i + H, 1 \le i \le p \). Thus for each \( 1 \le i \le p \), there is \( h_i \in H \) such that \( a_i = k_i + h_i \). But \( |H| = m < p \). By the pigeonhole principle there are two different indices, \( r \) and \( s \), such that \( h_r = h_s \). Thus \( a_r - a_s = k_r - k_s \in K \). Hence \( a_r \) and \( a_s \) are in the same coset modulo \( K \). This proves the theorem.

**Theorem 3.2.** If \( p \) is an odd prime and \( C(p^t) \setminus \{ 0 \} = MS \) is a splitting, then either \( M \) or \( S \) contains only elements relatively prime to \( p \).

**Proof.** Assume the contrary, that there are \( m, s \) such that \( m \in M, s \in S \), and \( p|m, p|s \). Then let

\[
G = \{ g : g \in C(p^t), \ (g, p) = 1 \}, \quad A = \{ a : a \in M, \ (a, p) = 1 \},
\]

and

\[
B = \{ b : b \in S, \ (b, p) = 1 \}.
\]
From the splitting $C(p^t) \setminus \{0\} = MS$ we have a multiplicative factorization $G = AB$. Note that $G$ is a cyclic group of order $p^{t-1}(p - 1)$. Thus according to Theorem 3.1 either $A$ or $B$ contains at least two elements from the same coset modulo the subgroup of order $p$. This subgroup consists of the elements $1, p^{t-1} + 1, 2p^{t-1} + 1, \ldots, (p - 1)p^{t-1} + 1$. Thus we may assume, without loss of generality, that $M$ contains the distinct elements $(ip^{t-1} + 1)u$ and $(jp^{t-1} + 1)u$, where $0 \leq i < j \leq p - 1$ and $(u, p) = 1$. Since $p|s$,

$$[(ip^{t-1} + 1)u] s \equiv [(jp^{t-1} + 1)u] s \pmod{p^t},$$

which contradicts the assumption that $C(p^t) \setminus \{0\} = MS$ is a splitting.

4. The direct sum of isomorphic copies. From the exact sequences

$$\{0\} \to \bigoplus_{i=1}^{t-1} H \to \bigoplus_{i=1}^t H \to H \to \{0\},$$

$2 \leq t \leq n$, it follows that if $M$ splits $H$ nonsingularly then $M$ splits $\bigoplus_{i=1}^n H$ for each positive integer $n$.

The next result shows that if $M$ splits $\bigoplus_{i=1}^n H$ singularly, then $n$ cannot be arbitrarily large.

**Theorem 4.1.** If $M$ splits $G = \bigoplus_{i=1}^n H$ singularly, then $2n+1 < |M||H|$.

**Proof.** Assume that $M$ splits $G = \bigoplus_{i=1}^n H$ singularly with splitting set $S$. If $p_1, \ldots, p_r$ are the different prime divisors of $|H|$, then $H$ is the direct sum of the $p_1 \ldots, p_r$-groups $H_1, \ldots, H_r$: $H = H_1 \oplus \cdots \oplus H_r$.

Furthermore, by the fundamental theorem of abelian groups, each $H_i$ is the direct sum of cyclic groups whose orders are powers of $p_i$, say orders $q_{i1}, \ldots, q_{ir}$: $H_i = H_1 \oplus \cdots \oplus H_r$.

Letting $t_i = q_{i1}q_{i2} \cdots q_{ir}$ we have $H = \bigoplus_{i=1}^t C(t_i)$ and therefore

$$G = \bigoplus_{j=1}^n H = \bigoplus_{j=1}^n \bigoplus_{i=1}^l C(t_i) = \bigoplus_{i=1}^n \bigoplus_{j=1}^l C(t_i).$$

We shall view $G$ as the sum

$$C(t_1) \oplus \cdots \oplus C(t_j) \oplus C(t_2) \oplus \cdots \oplus C(t_2) \oplus \cdots \oplus C(t_1) \oplus \cdots \oplus C(t_1),$$

where each $C(t_j)$ appears $n$ times. Thus each element in $G$ is an $nl$-tuplet.

Since $M$ splits $G$ singularly, one of $p_1, \ldots, p_r$, say $p_1$, divides an element of $M$. Thus for some integer $v$, $p_1v \in M$. Since $p_1$ divides $q_{11}$, it follows that $p_1$ divides $t_1$. Let $t_1 = p_1w$ and let $m_1 = p_1v$.

Consider the set of elements in $G$ of the form $(c, d_2w, \ldots, d_nw, 0, \ldots, 0)$, where $(c, t_1) = 1$ and $0 \leq d_j \leq p_1 - 1$. There are $\varphi(t_1)p_1^{n-1}$ such elements. Each of these
elements is of the form \( ms, m \in M, s \in S \). Let \( s = (x_{11}, \ldots, x_{1n}, \ldots, x_{l1}, \ldots, x_{ln}) \).

Then we have
\[
\begin{align*}
mx_{11} & \equiv c, & mx_{12} & \equiv d_2w, & \ldots, & mx_{1n} & \equiv d_nw \pmod{t_1}, \\
mx_{j1} & \equiv 0, & mx_{j2} & \equiv 0, & \ldots, & mx_{jn} & \equiv 0 \pmod{t_j}, & 2 \leq j \leq l.
\end{align*}
\]

From the first congruence it follows that \( (m, t_1) = 1 \) and consequently \( (m, t_j) = 1, 2 \leq j \leq l \). Recalling that \( t_1 = p_1w \), we conclude that \( w \) divides \( x_{12}, x_{13}, \ldots, x_{1n} \).

Now, for a given \( s \in S \) there are \( |M| \) elements in \( G \) of the form \( ms \). There are therefore at least \( \varphi(t_1)p_1^{n-1}/|M| \) elements in \( S \) that satisfy the above congruences. For each such \( s \)
\[
m_1s = (p_1v)s = p_1v(x_{11}, \ldots, x_{ln}) = (p_1v_{11}, 0, \ldots, 0).
\]

Thus \( \varphi(t_1)p_1^{n-1}/|M| \leq t_1/p_1 \), or \( \varphi(t_1)p_1^n \leq |M|t_1 \). If \( t_1 > 2 \), then we have \( 2 \leq \varphi(t_1), 2 \leq p_1 \), and \( t_1 \leq |H| \); thus \( 2^{n+1} \leq |M| |H| \). When \( t_1 = 2, G = C(2) \oplus \cdots \oplus C(2) \), which has no singular splitting. This concludes the proof.

The multiplier set \( M = \{1, 2, \ldots, k\} \) always splits \( C(k + 1) \) with splitting set \( \{1\} \). If this splitting is nonsingular then \( M \) splits any group \( G = C(((k + 1)^{a_1}) \oplus \cdots \oplus C((k + 1)^{a_n}) \).

In the singular case, as \([1]\) proved, if \( M \) splits \( G \) then \( G = C(k + 1) \).

Similarly, \( M \) always splits \( C(2k + 1) \) with splitting set \( \{-1, 1\} \). Thus in the nonsingular case \( M \) splits any group of the form \( G = C(((k + 1)^{a_1}) \oplus \cdots \oplus C((2k + 1)^{a_n}) \).

In \([14]\) it was shown that if \( 2k + 1 \) is not a power of a prime \( \equiv 1 \pmod{6} \) and \( M \) splits \( G \) singularly, then \( G = C(2k + 1) \). With the aid of Theorem 3.2 of this paper we now remove this exception.

Let \( t = lk + 1 \). It is clear that if \( M \) splits \( C(t) \) nonsingularly, then it splits each group \( G = C(t^a_1) \oplus \cdots \oplus C(t^a_n) \). From the exact sequences
\[
\{0\} \longrightarrow C(t^{a_i-1}) \oplus \bigoplus_{i=1 \atop i \neq j} C(t^{a_i}) \longrightarrow \bigoplus_{i=1}^{r} C(t^{a_i}) \longrightarrow C(t) \longrightarrow \{0\},
\]

\( 2 \leq r \leq n \), it follows that if \( M \) splits \( G \) and \( n \geq 2 \), then \( M \) splits \( C(t) \oplus C(t) \) even if the original splitting is singular. But the next theorem shows that \( M \) does not split this group singularly.

**THEOREM 4.2.** \( M = \{1, 2, \ldots, k\} \) does not split \( C(lk+1) \oplus C(lk+1) \) singularly.

**PROOF.** Assume the contrary, that \( M \) splits \( C(lk+1) \oplus C(lk+1) \) singularly. Let \( p_1, \ldots, p_r \) be the different prime divisors of elements of \( M \) and \( lk + 1 = uv \), where the prime divisors of \( u \) come from among \( p_1, \ldots, p_r \) and the prime divisors of \( v \) do not. Theorem 1.2.5 of \([5]\) shows that if \( M \) splits \( C(lk+1) \oplus C(lk+1) \), then it splits \( C(u) \oplus C(u) \) purely singularly.

Note that there exists an integer \( a \) such that \( a|u, 1 < a \leq k \), and \( k < a^2 \). Indeed, let \( a \) be the greatest proper divisor of \( u \) which is not greater than \( k \). If \( k < a^2 \) then we are done. So we may assume that \( a \leq \sqrt{k} \). Since \( a \) is a proper divisor of \( u \), at least one of the numbers \( ap_1, ap_2, \ldots, ap_r \), say \( ap_1 \), divides \( u \). By the definition of
a it follows that \( ap_1 > k \), that is, \( p_1 > k/a \geq \sqrt{k} \). Thus \( k < p_1^2 \). Since the splitting is purely singular, \( p_1 \leq k \), that is, \( p_1 \) can play the role of \( a \).

Select \( b \) such that \( u = ab \) and consider the \( a^2 \) elements \((ib+1, jb), 0 \leq i, j \leq a-1\). For each of these elements there exist \( m \in M \) and \( s \in S \) such that \((ib+1, jb) = ms\). Since \( a^2 > |M| \) there are \( m \in M \) and \( s', s'' \in S \) such that \( ms = (ib+1, jb), ms' = (i'b+1, j'b), (i, j) \neq (i', j') \), and \( s \neq s' \). If \( s = (x_1, x_2) \) and \( s' = (x_1', x_2') \), then \( mx_1 \equiv ib + 1, mx_1' \equiv i'b + 1, mx_2 \equiv jb, mx_2' \equiv j'b \) (mod \( u \)). From the first congruence we have \((m, b) = 1\) and so, from the last two, \( b|x_2 \) and \( b|x_2' \). From the first two we get \( x_1 \equiv x_1' \) (mod \( b \)). Thus \( x_1 = db + h, x_2 = bt, x_1' = d'b + h, \) and \( x_2' = bt' \). Consequently, \( as = a(x_1, x_2) = a(db + h, bt) = (ah, 0) \) and \( as' = a(x_1', x_2') = a(d'b + h, bt') = (ah, 0) \), which is a contradiction since \( s \neq s' \). This concludes the proof.

The main result of [11] is: If \( M = \{1, 2, \ldots, k\} \) splits \( C(lk + 1) \), and \( l > 3 \), then \( l > k + 2 \). Combining this with the previous theorem, we get the following result.

**Corollary.** If \( 2 < l < k + 2 \), then \( M = \{1, 2, \ldots, k\} \) does not split \( C(lk + 1) \oplus \cdots \oplus C(lk + 1) \).

**Proof.** An argument like that used in the proof of Theorem 4.2 shows that \( M \) does not split our group singularly. In the nonsingular case \( M \) splits our group if and only if it splits \( C(lk + 1) \). But, according to the cited result, \( M \) cannot split \( C(lk + 1) \).

**Acknowledgments.** The author would like to thank the referee for valuable suggestions.

**References**

14. _, Some problems on splittings of groups, Aequationes Math. 30 (1986), 70–79.

**Department of Civil Engineering Mathematics, Technical University of Budapest, 1111 Budapest, Stóczek u 2, Hungary**

*Current address:* Department of Mathematical Sciences, The University of Dundee, Dundee DD1 4HN, Scotland, U.K.