SPLITTING GROUPS BY INTEGERS

W. HAMAKER AND S. STEIN

ABSTRACT. A question concerning tiling Euclidean space by crosses raised this algebraic question: Let $G$ be a finite abelian group and $S$ a set of integers. When do there exist elements $g_1, g_2, \ldots, g_n$ in $G$ such that each nonzero element of $G$ is uniquely expressible in the form $sg_i$ for some $s$ in $S$ and some $g_i$? The question is answered for a broad (but far from complete) range of $S$ and $G$.

Let $G$ be a finite abelian group and $S = \{s_1, s_2, \ldots, s_k\}$ a set of $k$ distinct integers. If there are elements $g_1, g_2, \ldots, g_n$ in $G$ such that each nonzero element of $G$ is uniquely expressible in the form $sg_i, 1 \leq i \leq k, 1 \leq j \leq n$, we will say that $S$ splits $G$. The set $\{g_1, \ldots, g_n\}$ is a splitting set. The cases $S = \{1, 2, \ldots, k\}$ and $S = \{-1, -2, \ldots, -k\}$ arise in the case of tiling Euclidean space by certain starbodies (see [2] and [3]). In [1] it was shown that $S = \{1, 3, 27\}$ splits no finite abelian group. If each $s_i \in S$ is relatively prime to $|G|$, the order of $G$, we call the splitting nonsingular. Throughout we will assume that all groups have at least two elements.

Theorem 1. Let $S$ split the groups $A$ and $B$ such that the splitting of $A$ is nonsingular. Let $0 \rightarrow A \xrightarrow{\alpha} G \xrightarrow{\beta} B \rightarrow 0$ be an exact sequence (kernel $\beta =$ image $\alpha$, $\alpha$ one-one, $\beta$ onto). Then $S$ splits $G$.

Proof. Let $a_1, a_2, \ldots, a_p$ be a splitting set in $A$, and $b_1, b_2, \ldots, b_q$ be a splitting set in $B$. For each $n, 1 \leq n \leq q$, select $g_n \in G$ such that $\beta(g_n) = b_n$. We assert that the set

$$
\{\alpha(a_j) : 1 \leq j \leq p\} \cup \{\alpha(a) + g_n : a \in A - \{0\}, 1 \leq n \leq q\}
$$

is a splitting set for $G$.

To begin, let $U = \{a_1, \ldots, a_p\}$ and $V = \{g_1, \ldots, g_n\}$. Then we wish to show first that $G - \{0\} = S(\alpha(U) \cup (\alpha(U) + V))$. Noting that $SV \cup \{0\}$ is a complete set of coset representatives for $G$ mod $\alpha(A)$, we have
G - \{0\} = (\alpha(A) - \{0\}) \cup (\alpha(A) + SV) = S(\alpha(U)) \cup (\alpha A + SV).

Now, since \(S\) splits \(A\) in a nonsingular manner, \(SA = A\), hence \(S(\alpha A) = \alpha A\).

Also, for any sets \(X\) and \(Y\) in \(G\) such that \(SX = X\), we have \(X + SY = SX + SY\). Thus

\[ G - \{0\} = S(\alpha(U)) \cup (\alpha A + SV) = S(\alpha(U)) \cup S(\alpha A + V) \]

\[ = S(\alpha(U)) \cup (\alpha A + V), \]

as desired.

The uniqueness of the representation follows from the fact that the set

\[(1) \text{ contains } \frac{|A| - 1}{k} + \frac{|B| - 1}{k} + \frac{(|A| - 1)(|B| - 1)/k}{2},\]

elements.

The following two corollaries are of special interest.

**Corollary 1.** Let \(S\) split the groups \(A\) and \(B\) in such a way that the splitting of \(A\) is nonsingular. Then \(S\) splits the product \(A \times B\).

**Corollary 2.** Let \(S\) split \(C(q)\) in a nonsingular manner. Then \(S\) splits \(C(q^n)\) for each positive integer \(n\).

**Proof.** There is an exact sequence \(0 \rightarrow C(q) \rightarrow C(q^{n+1}) \rightarrow C(q^n) \rightarrow 0\). Theorem 1, combined with an induction on \(n\), establishes the Corollary.

The two corollaries, together with the fundamental theorem of abelian groups, yield the following theorem.

**Theorem 2.** Let \(p\) be an odd prime integer. Let \(S = \{1, 2, \ldots, p - 1\}\) or \(\{\pm 1, \pm 2, \ldots, \pm(p - 1)/2\}\). Then \(S\) splits any abelian group whose order is a power of \(p\).

[As [2] or [3] show, Theorem 2 implies, for example, that a \((p - 1)/2\) cross tiles Euclidean \(n\) space if \(n(p - 1) + 1\) is a power of \(p\), say \(p^b\), in at least as many geometrically inequivalent ways as there are nonisomorphic abelian groups of order \(p^b\).]

The next theorem is sort of a converse to Theorem 1.

**Theorem 3.** Let \(0 \rightarrow A \xrightarrow{\alpha} G \xrightarrow{\beta} B \rightarrow 0\) be an exact sequence of groups. Assume that \(S\) splits \(G\). If each \(s_i\) in \(S\) is relatively prime to \(|B|\), then \(S\) splits \(A\). If each \(s_i\) in \(S\) is relatively prime to \(|A|\), then \(S\) splits \(B\).

**Proof.** We begin by proving the first assertion. Let \(T = \{g_1, g_2, \cdots, g_n\}\) be the splitting set of \(G\). We assert that \(\alpha(A) \cap T\) is a splitting set for \(\alpha(A)\). (Hence \(\alpha^{-1}(\alpha(A) \cap T)\) would be a splitting set for \(A\)).
We establish first that
\[ \alpha(A) - \{0\} = S(\alpha(A) \cap T), \]
or, equivalently,
\[ \alpha(A) \cap ST = S(\alpha(A) \cap T). \]
Clearly, \( \alpha(A) \cap ST \supseteq S(\alpha(A) \cap T) \). To show that \( S(\alpha(A) \cap T) \supseteq \alpha(A) \cap ST \), note that for \( s \in S \) and \( t \in T \)
\[ st \in \alpha(A) \Rightarrow s\beta(t) = \beta(st) = 0 \Rightarrow \beta(t) = 0, \]
since \( (s, |B|) = 1 \). Hence \( t \in \alpha(A) \) and \( \alpha(A) \cap ST \subseteq S(\alpha(A) \cap T) \).
Thus every element of \( \alpha(A) - \{0\} \) is representable in the form \( sg \) where \( s \in S \) and \( g \in \alpha(A) \cap T \). Showing that this representation is unique is straightforward.

The second assertion in the theorem is an immediate consequence of the fact that a homomorphic image of \( G \) is isomorphic to a subgroup of \( G \). This reduces the second case to the first. This concludes the proof.

The assumption in Theorem 3 that \( (s_i, |B|) = 1 \) cannot be removed. To see this, consider \( S = \{1, 2, 3\} \) and an exact sequence \( 0 \rightarrow C(2) \rightarrow C(4) \rightarrow C(2) \rightarrow 0 \).

Theorem 3, combined with Corollaries 1 and 2, yield the following reduction of the problem of determining all nonsingular splittings.

**Theorem 4.** Let \( G \) be a finite abelian group and \( S = \{s_1, s_2, \ldots, s_k\} \) a set of integers with each \( s_i \) relatively prime to \( |G| \). Then \( S \) splits \( G \) if and only \( S \) splits \( C(p) \) for each prime \( p \) that divides \( |G| \).

**REFERENCES**

   MR 36 #2517.

DEPARTMENT OF MATHEMATICS, DREXEL UNIVERSITY, PHILADELPHIA, PENNSYLVANIA 19104

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, DAVIS, CALIFORNIA 95616