PACIFIC JOURNAL OF MATHEMATICS
Vo. 22, No. 3, 1967

FACTORING BY SUBSETS

S. K. STEIN

If a group G is the direct product of two of its subgroups, A and B, then every element of G is uniquely expressible in the form $ab, a \in A, b \in B$. In 1942, G. Hajós, in order to solve a geometric problem posed by Minkowski, introduced the notion of the direct product of subsets. He said that the group G is the direct product of two of its subsets, A and B, if each element of G is uniquely expressible in the form $ab, a \in A, b \in B$, and showed that under certain circumstances one of the sets is a group.

While Hajós's work grew out of a question concerning the partition of Euclidean n-dimensional space into congruent cubes, the present paper grew out of a question concerning partitions into congruent "crosses" and is concerned primarily with the existence of factorizations of the semigroup of integers modulo m into subsets A and B, of which A is prescibed as $\{1, 2, \cdots, k\}$ or $\{\pm 1, \pm 2, \cdots, \pm k\}$. The first three sections are algebraic and geometric, while the last two sections are number-theoretic.

Let A and B be subsets of a groupoid G. We will denote by AB the set $\{ab \mid a \in A, b \in B\}$. If each element of AB is uniquely expressible in the form $ab, a \in A, b \in B$, then we say that AB has the factoring (A, B) or briefly, $AB = (A, B)$. For instance, if G is a group, A is a subgroup of G, and B is a set of representatives of the right cosets of A in G, then $G = (A, B)$. The case when G is a finite abelian group and A and B are subsets of $G, G = (A, B)$, was examined in the classic paper of Hajós [3], later simplified by Szele [13] and Rédei [10].

When $AB = (A, B)$, there is no duplication among the elements $ab, a \in A, b \in B$. The opposite situation, when AB is "small" and there is therefore a great deal of duplication, has also been studied. See for instance Kemperman [6], [7].

For the most part the groupoid G that will concern us is S_n the multiplicative semigroup of the integers modulo n. We will be interested in factorizations $S_n - \{0\} = (A, B)$, where A is prescribed. Such factorizations, as we will show in § 2, are intimately connected with the existence of tessellations of Euclidean space by translates of certain finite collections of cubes. Before restricting the groupoid to S_n, we develop in § 1 some results that hold more generally.

1. Algebraic preliminaries.

If G is a groupoid and X is a