PACIFIC JOURNAL OF MATHEMATICS
Vol. 140, No. 1, 1989

A NEW PROOF OF RÉDEI'S THEOREM

KERESZTÉLY CORRÁDI AND SÁNDOR SZABÓ

If a finite abelian group is expressed as the product of subsets each of which has a prime number of elements and contains the identity element, then at least one of the factors is a subgroup. This theorem was proved by L. Rédei in 1965. In this paper we will give a shorter proof.

1. Introduction. Let G be a finite abelian group written multiplicatively, and let $A_1, \ldots, A_n$ be subsets of G. If each $g \in G$ is uniquely expressible in the form $g = a_1 \cdots a_n$, $a_1 \in A_1, \ldots, a_n \in A_n$, then we say that $G = A_1 \cdots A_n$ is a factorization of G. If each A_i contains the identity element, we speak of a normed factorization.

The subset $\{1, g, g^2, \ldots, g^{q-1}\}$ will be denoted by $[g, q]$ and called the simplex generated by g with length q, provided that q is a positive integer not greater than the order of g.

Let H be the p-Sylow subgroup of G and K its direct factor complement. We denote the order of K by p'. Each $g \in G$ can be expressed uniquely in the form $g = hk$, $h \in H$, $k \in K$. The element h will be called the p-part of g and denoted by $g|_p$, and the element k will be denoted by $g|_{p'}$.

We will use these two known facts.

(1) The nth cyclotomic polynomial is irreducible over the mth cyclotomic field if m is prime to n.

(2) Let $n > 1$ be an integer and p its smallest prime factor. Then any set of fewer than p nth roots of unity is linearly independent over the field of rationals.

For a short proof see [5].

Proving a conjecture made by H. Minkowski in 1896, G. Hajós in 1941 showed that in a simplex factorization of a finite abelian group at least one of the simplices must be a subgroup.

It may be assumed without loss of generality that in this theorem the lengths of the simplices are primes. So the following result of L. Rédei is a broad generalization of it.