A Book of Abstract Algebra | (2nd Edition)

Problem

As a provisional definition, let us call a finite abelian group “decomposable” if there are elements $a_1, \ldots, a_n \in G$ such that:

(DI) For every $x \in G$, there are integers $k_1, \ldots, k_n$ such that $x = a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n}$. (D2)

If there are integers $l_1, \ldots, l_n$ such that

$a_1^{l_1} a_2^{l_2} \cdots a_n^{l_n} = e$ then $a_1^{l_1} = a_2^{l_2} = \cdots = a_n^{l_n} = e$.

If (D_1) and (D_2) hold, we will write $G = [a_1, a_2, \ldots, a_n]$. Assume this in parts 1 and 2.

Let G' be the set of all products $a_2^{l_2} \cdots a_n^{l_n}$, as $l_2, \ldots, l_n$ range over $\mathbb{Z}$.

Prove that G' is a subgroup of G, and $G' = [a_2, \ldots, a_n]$.

Step-by-step solution

Step 1 of 3

Assume that a finite abelian group G, of order $p^k m$, is decomposable. That is, if $a_1, \quad, a_n \in G$ and both the conditions $D1$, $D2$ holds, then $G = [a_1, a_2, \quad, a_n]$.

Let G' be the set of all products $a_2^{l_2} a_3^{l_3} \quad a_n^{l_n}$, as $l_2, l_3, \ldots, l_n$ range over integers. Objective is to prove that G' is a subgroup of G, and $G' = [a_2, \quad, a_n]$.

One step test: If H is a nonempty subset of group G, then H will be subgroup of G if and only if for all $a, b \in H$

$ab^{-1} \in H$.

Comment

Step 2 of 3

Since G' be the set of all products $a_2^{l_2} a_3^{l_3} \quad a_n^{l_n}$, where $l_2, l_3, \ldots, l_n$ are integers. Therefore, the set G' is closed under multiplication. Since $l_2, l_3, ..., l_n$ are arbitrary integers, so $-l_2, -l_3, ..., -l_n$ also. This shows that inverse of each $a_i^{l_i}$ will be $a_i^{-l_i} \in G'$.

Then again by the multiplication closed property,

$$a_j^{l_j} \cdot a_i^{-l_i} \in G',$$

for some *i* and *j*. Thus, any set generated by some set of elements forms a subgroup. Now, by the definition

$a_1^0 \cdot a_2^{l_2} a_3^{l_3} \quad a_n^{l_n} = e$ implies $a_i^{l_i} = e$.

So, $G' = [a_2, \quad , a_n]$.

Comment

Step 3 of 3

Hence, G' is a subgroup of *G*, and $G' = [a_2, \quad , a_n]$.

Comment