A Book of Abstract Algebra | (2nd Edition)

Chapter 16, Problem 2EO

Problem

The purpose of this exercise is to prove a property of cosets which is needed in Exercise Q. Let G be a finite abelian group, and let a be an element of G such that ord(a) is a multiple of ord(x) for every $x \in G$. Let $H = \langle a \rangle$. We will prove:

For every $x \in G$, there is some $y \in G$ such that $Hx = Hy$ and ord(y) = *ord*(Hy).

This means that every coset of H contains an element y whose order is the same as the coset's order.

Let x be any element in G, and let ord (a) = t, ord(x) = s, and ord (Hx) = r.

Deduce from our hypotheses that r divides s, and s divides t.

Thus, we may write $s = ru$ and $t = su$, so in particular, $t = ruu$.

Step-by-step solution

Step 1 of 4

Consider that G is a finite abelian group. Let $a, x \in G$ and $H = \langle a \rangle$ is a subgroup of G. Suppose that order of the elements are:

$$\begin{aligned}
&\operatorname{ord}(a) = t,\\
&\operatorname{ord}(x) = s,\\
&\operatorname{ord}(Hx) = r.
\end{aligned}$$

Note that r is the least positive integer such that x^r equals some power of a, say $x^r = a^m$.

Objective is to conclude from the hypothesis that r divides s, and s divides t.

Comment

Step 2 of 4

Observe that the Hx denotes the coset of the quotient group G/H. By the definition of quotient group, one have that the identity of group G/H is equal to *H*.

Since $\operatorname{ord}(Hx) = r$, so

$$\begin{aligned}(Hx)^r &= H \\ Hx^r &= H.\end{aligned}$$

Now find the $s\text{th}$ power of coset Hx as:

$$\begin{aligned}(Hx)^s &= Hx^s \\ &= He \\ &= H.\end{aligned}$$

Second step is obtained from the condition that,

$\operatorname{ord}(x) = s$, so $x^s = e$.

Comment

Step 3 of 4

The equation $(Hx)^s = H$ shows that *s* is a multiple of the order of coset Hx (because order is the least positive integer). Thus, $r \mid s$.

Since $\operatorname{ord}(a) = t$ and $\operatorname{ord}(x) = s$. Also from the hypothesis it is known that $\operatorname{ord}(a)$ is a multiple of $\operatorname{ord}(x)$ for every *x* in *G*. That is, *t* is a multiple of *s*. Thus, $s \mid t$.

Comment

Step 4 of 4

Hence, $r \mid s$ and $s \mid t$. Then by the definition of divisibility, there exist some integer *u* and *v* such that

$s = ru, t = sv$, or $t = ruv$.

Comment