A Book of Abstract Algebra | (2nd Edition)

Chapter 16, Problem 3EO

Bookmark

Show all steps: ON

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*.

Explain why $a^{mu} = e$, and why it follows that $mu = tz$ for some integer *z*. Then explain why $m = ruz$.

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:

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

Note that *r* is the least positive integer such that x^r equals some power of *a*, say $x^r = a^m$. Also *r* divides *s*, and *s* divides *t*.

Objective is to prove that $a^{mu} = e$, and it follows that $mu = tz$ for some integer *z*. Also explain that $m = rvz$.

Comment

Step 2 of 4

From the hypothesis, one have

$x^r = a^m$, and $x^s = e$ (as $\operatorname{ord}(x) = s$).

Also *r* divides *s*, so for some integer *u*, $s = ru$.

Now consider the $s\text{th}$ power *x* as:

$$\begin{aligned} x^s &= x^{ru} \\ &= \left(x^r\right)^u \\ &= \left(a^m\right)^u \\ &= a^{mu}. \end{aligned}$$

Since $x^s = e$, therefore

$a^{mu} = e\cdot$

Comment

Step 3 of 4

Since $\operatorname{ord}(a) = t$ and order is the least positive integer to give an identity. Therefore,

$t \mid mu$.

So, mu is a multiple of *t*. That is, for some integer *z*,

$mu = tz$.

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

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

Substitute the value of *t* in $mu = tz$ and get, $mu = ruvz.$. Now, by the cancellation law,

$m = rvz$.

Comment

Step 4 of 4

Hence, $a^{mu} = e$, and it follows that $mu = tz$ for some integer *z*. Also, $m = rvz$.

Comment