From Mathematics to Generic Programming

Brooks Mershon

March 2017

6.7

Solution.

We recall that a cyclic group G has an element a such that for any element b, there is an integer n where

$$b = a^n$$

Now, if we have a subgroup H which is the singleton set $\{1\}$, then this trivial subgroup of G is generated by its only element.

If instead we have a nontrivial subgroup H, then let m be the smallest positive integer such that $a^m \in G$ (this excludes considering the identity element.

Now consider an arbitrary element $b \in H$. We know $b = a^n \in G$ for some n, since H is a subgroup of G. We can certainly say that $n = l \cdot m + r$ for integers l and r, where r is the remainder when we attempt to divide n by m. So $0 \leq r \geq m$. What we shall do is use the assumption that m is the smallest integer such that $a^m \in G$ along with some algebraic manipulation of our expression for n in order to show that $a^m \in H$ is a generating element which may be used to generate an arbitrary $b \in H$ by raising a^m to some power.

With some substitution and rearranging, we have

$$a^n = a^{lm+r} = (a^m)^l a^r$$

This much we achieved by substituting and observing properties of exponents. Now for some more rearrangement:

$$\begin{aligned} a^r &= \frac{a^n}{(m)^l} = a^{n-ml} = \left(a^{-m}\right)^l a^n \\ &= (a^m)^{-l} a^n \end{aligned}$$

Now, we know that since H is a subgroup, the inverse of a^m must be in H. And because a group is closed under powers, we know powers of the inverse of a^m must be in H; therefore, $(a^m)^{-l} \in H$. But our arbitrary $b = a^n$ is also in H. Under the closure property of groups, $(a^m)^{-l} a^n$ must be in H as well.

Since we have constructed our remainder r such that $0 \leq r \geq m$, and we assumed that m was the smallest positive integer such that a^m is in H. This implies $r = 0$, otherwise we would contradict our assumption about m.

Immediately then, we have that $n = lm$ and therefore

$$b = a^n = a^{lm} = (a^m)^l$$

Since we let b be an arbitrary element in H, we know any b in H may be generated by an element in H which we know can be constructed by raising it to some power l. So *any* subgroup of a cyclic group is cyclic.