From Mathematics to Generic Programming

Brooks Mershon

March 2017

6.8

Solution.

Let $b = g^n$ for some generating element g in G. Let $a = g^m$.

We want to show that our arbitrary a and b chosen from a cyclic group will satisfy

$$a \circ \underline{=} b \circ a$$

We can use the Commutativity of Powers (6.1) to show that a cyclic group is indeed *abelian*.

$$a \circ b = g^n g^m = g^m g^n = ba = b \circ a$$

This holds for any a and b, as a and b were chosen arbitrarily.