Group Properties

Proof showing that taking the operation of three elements and then the inverse of the result is the same as taking the inverses of each element and then performing the group operations.

By Joseph Pousada
December 24, 2013

Groups have certain basic properties by definition. As a result of this, we are able to construct rules and relationships with the elements in the groups. The definition of a group is:

"A group is an ordered pair $(G,\star)$ where G is a set and $\star$ is a binary operation on G satisfying the following axioms:
(i) $(a\star b)\star c = a\star(b\star c)$, for all $a, b, c \in G$, i.e., $\star$ is associative,
(ii) there exists and element e in G, called an identity of G, such that for all $a\in G$ we have $a\star e = e\star a = a$,
(iii) for each $a\in G$ there is an element a^{-1} of G, called an inverse of a, such that $a\star a^{-1} = a^{-1}\star a = e$."(Dummit, D. S., & Foote, R. M.,pgs 16 & 17, (2004)

We can now use these basic properties of the definition of a group to show via direct proof that $(a_1\star a_2\star a_3)^{-1} = a_3^{-1}\star a_2^{-1}\star a_1^{-1}$. We first assume that G is a group and that the elements $a_1, a_2, a_3, b_1 \in G$.

Given $(a_1\star a_2\star a_3)^{-1}$ & $(a_3^{-1}\star a_2^{-1}\star a_1^{-1})$ are part of the group then the associative property where for all $a, b, c\in G$ $(a\star b)\star c = a\star(b\star c)$ as well as a^{-1} is the inverse of a and a is the inverse of a^{-1} (sometimes noted as $(a^{-1})^{-1} = a$) apply. We can set all the values so that

$((a_1\star a_2\star a_3)^{-1})\star((a_3)\star(a_2)\star(a_1)) = 1$

If we add $(a_1)^{-1}$ to both sides of the equation we get:

$((a_1\star a_2\star a_3)^{-1})\star((a_3)\star(a_2)\star(a_1))\star(a_1^{-1}) = 1\star(a_1^{-1})$

Since these are all elements of a group we can use the associative property and the identity property to state:

$((a_1\star a_2\star a_3)^{-1})\star((a_3)\star(a_2)\star((a_1)\star(a_1^{-1})) = (a_1^{-1})$

Then we use the property of inverses for groups to state

$((a_1\star a_2\star a_3)^{-1})\star((a_3)\star(a_2))\star(1) = (a_1^{-1})$

Now we can continue by adding (a_2^{-1}) to both sides of the equation to get:

$((a_1\star a_2\star a_3)^{-1})\star((a_3)\star(a_2))\star(1)\star(a_2^{-1}) = (a_1^{-1})\star(a_2^{-1})$

We again use the associative property and the identity property to state

$((a_1\star a_2\star a_3)^{-1})\star(a_3)\star((a_2)\star(a_2^{-1})) = (a_1^{-1})\star(a_2^{-1})$

Then we use the property of inverses for groups to state

$((a_1\star a_2\star a_3)^{-1})\star(a_3)\star(1) = (a_1^{-1})\star(a_2^{-1})$

Now we can continue by adding $\left(a_3^{-1}\right)$ to both sides of the equation to get:

$$\left(\left(a_1 \star a_2 \star a_3\right)^{-1}\right) \star \left(a_3\right) \star (1) \star \left(a_3^{-1}\right) = \left(a_1^{-1}\right) \star \left(a_2^{-1}\right) \star \left(a_3^{-1}\right)$$

We again use the associative property and the identity property to state

$$\left(\left(a_1 \star a_2 \star a_3\right)^{-1}\right) \star \left(\left(a_3\right) \star \left(a_3^{-1}\right)\right) = \left(a_1^{-1}\right) \star \left(a_2^{-1}\right) \star \left(a_3^{-1}\right)$$

Then we use the property of inverses for groups to state

$$\left(\left(a_1 \star a_2 \star a_3\right)^{-1}\right) \star (1) = \left(a_1^{-1}\right) \star \left(a_2^{-1}\right) \star \left(a_3^{-1}\right)$$

Now we can use the identity property to state

$$\left(\left(a_1 \star a_2 \star a_3\right)^{-1}\right) = \left(a_1^{-1}\right) \star \left(a_2^{-1}\right) \star \left(a_3^{-1}\right)$$

Therefore we can state that $\left(\left(a_1 \star a_2 \star a_3\right)^{-1}\right) = \left(a_1^{-1}\right) \star \left(a_2^{-1}\right) \star \left(a_3^{-1}\right)$.

References

Dummit, D. S., & Foote, R. M. (2004). Abstract algebra. Hoboken, NJ: Wiley.