Introduction to Modern Algebra

Part I. Groups and Subgroups

I.4. Groups

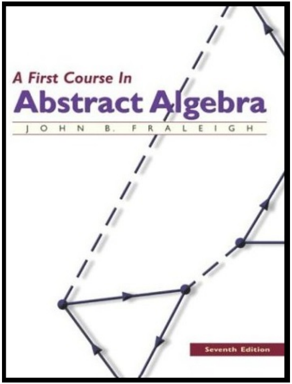

Table of contents

Theorem 4.15

Theorem 4.15. If $\langle G, *\rangle$ is a group, then (1) $a * c = b * c \implies b = c$ and (2) $b * a = c * a \implies b = c$ for all $a, b, c \in G$. These properties are called the left and right cancellation laws, respectively.

Proof. Let $a, b, c \in G$ and let a' be the inverse of a. Then $a * b = a * c \implies a' * (a * b) = a' * (a * c)$. By associativity, $(a' * a) * b = (a' * a) * c$ and $e * b = e * c$ (since a' is the inverse of a) and $b = c$ since e is the identity of G. Right cancellation follows similarly. □

Theorem 4.15

Theorem 4.15. If $\langle G, * \rangle$ is a group, then (1) $a * c = b * c \implies b = c$ and (2) $b * a = c * a \implies b = c$ for all $a, b, c \in G$. These properties are called the left and right cancellation laws, respectively.

Proof. Let $a, b, c \in G$ and let a' be the inverse of a. Then $a * b = a * c \implies a' * (a * b) = a' * (a * c)$. By associativity, $(a' * a) * b = (a' * a) * c$ and $e * b = e * c$ (since a' is the inverse of a) and $b = c$ since e is the identity of G. Right cancellation follows similarly. $\square$

Theorem 4.16

Theorem 4.16. If $\langle G, * \rangle$ is a group, then the equations $a * x = b$ and $y * a = b$ have unique solutions x and y for all $a, b \in G$.

Proof. First, consider $a* = b$. Then $a' * (a * x) = a' * b$ and $(a' * a) * x = a' * b$ by associativity, or $e * x = a' * b$ and hence $x = a' * b$ is a solution. To show uniqueness of solutions, suppose x_1 and x_2 are both solutions : $a * x_1 = a * x_2 = b$. Then by left cancellation (Theorem 4.15), $x_1 = x_2$ and the solution is unique. The result follows similarly for equation $y * a = b$. □

Theorem 4.16

Theorem 4.16. If $\langle G, * \rangle$ is a group, then the equations $a * x = b$ and $y * a = b$ have unique solutions x and y for all $a, b \in G$.

Proof. First, consider $a* = b$. Then $a' * (a * x) = a' * b$ and $(a' * a) * x = a' * b$ by associativity, or $e * x = a' * b$ and hence $x = a' * b$ is a̲ solution. To show uniqueness of solutions, suppose x_1 and x_2 are both solutions : $a * x_1 = a * x_2 = b$. Then by left cancellation (Theorem 4.15), $x_1 = x_2$ and the solution is unique. The result follows similarly for equation $y * a = b$. $\square$

Theorem 4.17a

Theorem. 4.17a. In group $\langle G, * \rangle$, there is only on element $e \in G$ such that $e * x = x * e = x$ for al $x \in G$.

Proof. Uniqueness of the identity of a binary operation was shown in Theorem 3.13. □

Theorem 4.17a

Theorem. 4.17a. In group $\langle G, * \rangle$, there is only on element $e \in G$ such that $e * x = x * e = x$ for al $x \in G$.

Proof. Uniqueness of the identity of a binary operation was shown in Theorem 3.13. □

Theorem 4.17b

Theorem. 4.17b. In group $\langle G, * \rangle$ for any given $a \in G$ there is only one element $a' \in G$ such that $a' * a = a * a' = e$. That is, inverses are unique.

Proof. Suppose that a' and a'' are both inverses of element $a \in G$. Then $a * a' = a * a'' = e$ and by left cancellation (Theorem 4.15), $a' = a''$. $\square$

Theorem 4.17b

Theorem. 4.17b. In group $\langle G, * \rangle$ for any given $a \in G$ there is only one element $a' \in G$ such that $a' * a = a * a' = e$. That is, inverses are unique.

Proof. Suppose that a' and a'' are both inverses of element $a \in G$. Then $a * a' = a * a'' = e$ and by left cancellation (Theorem 4.15), $a' = a''$. $\square$

Corollary 4.18

Corollary 4.18. Let G be a group. For all $a, b \in G$, we have $(a * b)' = b' * a'$.

Proof. We often denote the inverse of a as $a' = a^{-1}$. We have

$$\begin{aligned}
(a * b) * (b' * a') &= (a * b) * (b^{-1} * a^{-1}) \\
&= ((a * b) * b^{-1}) * a^{-1} \text{ by associativity} \\
&= (a * (b * b^{-1})) * a^{-1} \text{ by associativity} \\
&= (a * e) * a^{-1} \\
&= a * a^{-1} \\
&= e.
\end{aligned}$$

So $b^{-1} * a^{-1}$ is the inverse of $a * b$. □

Corollary 4.18

Corollary 4.18. Let G be a group. For all $a, b \in G$, we have $(a * b)' = b' * a'$.

Proof. We often denote the inverse of a as $a' = a^{-1}$. We have

$$\begin{array}{rcll} (a * b) * (b' * a') & = & (a * b) * (b^{-1} * a^{-1}) & \\ & = & ((a * b) * b^{-1}) * a^{-1} & \text{by associativity} \\ & = & (a * (b * b^{-1})) * a^{-1} & \text{by associativity} \\ & = & (a * e) * a^{-1} & \\ & = & a * a^{-1} & \\ & = & e. & \end{array}$$

So $b^{-1} * a^{-1}$ is the inverse of $a * b$. □